

THE MINIMAL REGULAR MODEL OF A FERMAT CURVE OF ODD SQUAREFREE EXPONENT AND ITS DUALIZING SHEAF

CHRISTIAN CURILLA AND J. STEFFEN MÜLLER

ABSTRACT. We construct the minimal regular model of the Fermat curve of odd squarefree composite exponent N over the N -th cyclotomic integers. As an application, we compute upper and lower bounds for the arithmetic self-intersection of the dualizing sheaf of this model.

CONTENTS

1. Introduction	2
Part I: The minimal regular model of Fermat curves of odd squarefree exponent	4
2. Preliminaries	4
2.1. Regularity	4
2.2. Blow-ups	5
2.3. Intersection theory on arithmetic surfaces	9
3. The local minimal regular model	10
3.1. The polynomial $\psi(X^m, Y^m)$	11
3.2. The blow-up of \mathcal{X} along $V(I)$	12
3.3. Resolving the singularities of $\tilde{\mathcal{X}}$	15
3.4. The configuration of the geometric special fiber of the local minimal regular model	21
4. The global minimal regular model	25
Part II: The arithmetic self-intersection of the relative dualizing sheaf on the minimal model of a Fermat curve of odd squarefree exponent	27
5. Bounding the arithmetic self-intersection of the relative dualizing sheaf on arithmetic surfaces	27
5.1. Arakelov intersection theory on arithmetic surfaces	27
5.2. Kühn's upper bound	27
5.3. Lower bounds	28
6. Computations on the local minimal regular model	29
6.1. Local extensions of cusps	29
6.2. Some vertical \mathbb{Q} -divisors and intersections	31
7. Bounds for $\bar{\omega}_{\mathfrak{f}_N}^2$	36

Date: May 17, 2016.

7.1. An upper bound for $\bar{\omega}_{\mathfrak{F}_N^{\min}}^2$	36
7.2. A lower bound for $\bar{\omega}_{\mathfrak{F}_N^{\min}}^2$	39
References	41

1. INTRODUCTION

In the history of number theory and arithmetic geometry, the study of the Fermat curve

$$(1.1) \quad F_N : X^N + Y^N = Z^N$$

of exponent $N \geq 3$ has played a prominent part. In this paper we consider the case of the Fermat curve F_N where N is squarefree, odd and composite.

For explicit computations and bounds in the arithmetic geometry of curves over number fields, one often needs to compute a regular model of the curve over the ring of integers. While it is sometimes possible to compute a regular model of a given curve X using, for instance, the computer algebra system **Magma**, the construction of regular models depending on a parameter is more involved. In the case of the Fermat curve $F_p/\mathbb{Q}(\zeta_p)$ of prime exponent $N = p \geq 3$ over the field of p -th cyclotomic numbers, the minimal regular model \mathfrak{F}_p^{\min} over $\mathbb{Z}[\zeta_p]$ was constructed by McCallum [Mc]. For other values of N , the minimal regular model \mathfrak{F}_N^{\min} of F_N over $\mathbb{Z}[\zeta_N]$ is not available in the literature.

In Part I of the present paper, we construct \mathfrak{F}_N^{\min} when N is squarefree, odd and composite by following the construction of \mathfrak{F}_p^{\min} due to McCallum. However, the non-prime case is much more complicated. It turns out that the only reducible fibers of \mathfrak{F}_N^{\min} lie above primes of $\mathbb{Z}[\zeta_N]$ dividing N , see Proposition 4.1. For such a prime \mathfrak{p} , the Zariski closure $\mathfrak{F}_{N,\mathfrak{p}}^0$ of F_N in \mathbb{P}_R^2 consists of a single component of multiplicity p , where p is the residue characteristic and R is the localization of $\mathbb{Z}[\zeta_N]$ with respect to \mathfrak{p} . Blowing up along this component, we obtain a normal model. The nonregular points of the latter can then be resolved by blow-ups, leading to a regular model of $F_N \times_{\mathbb{Z}[\zeta_N]} R$. The configuration of its special fiber is described in Theorem 3.13, which shows, in particular, that the model is minimal. The local regular models can then be glued to construct the minimal regular model \mathfrak{F}_p^{\min} . Note that we can recover McCallum's results as a special case of our construction, see Remark 3.14.

Once an explicit description of \mathfrak{F}_N^{\min} is available, several interesting arithmetic invariants of F_N can be computed, or at least bounded. These include some of the invariants appearing in the conjecture of Birch and Swinnerton-Dyer, and Arakelov-theoretic invariants. In Part II of the present article, we consider the latter, focusing on explicit bounds for the arithmetic self-intersection $\bar{\omega}_{\mathfrak{F}^{\min}}^2$ of the relative dualizing sheaf of \mathfrak{F}^{\min} , equipped with the Arakelov metric. The computation of such bounds was proposed in [La, p. 130] and [MB, §8.2].

If \mathcal{X} is an arithmetic surface defined over the ring of integers \mathcal{O}_K of a number field K such that the generic fiber X of \mathcal{X} has genus $g \geq 2$, then the arithmetic self-intersection $\bar{\omega}_{\mathcal{X}}^2$ of the relative dualizing sheaf of \mathcal{X} , equipped with the Arakelov metric, is one of the most important invariants of \mathcal{X} (or, if \mathcal{X} is the minimal regular model of X , of X). It is related to the Faltings height of X and several other invariants, see [Ja] for a summary. Lower bounds for $\bar{\omega}_{\mathcal{X}}^2$ are crucial in the context of the Bogomolov conjecture for curves, proved by Szpiro [Sz], Zhang [Zh1] and Ullmo [Ul]. However, an effective version of the Bogomolov conjecture, which in the function field case is known due to work of Zhang [Zh2] and Cinkir [Cin], is still an open problem in the number field case.

On the other hand, suitable upper bounds for $\bar{\omega}_X^2$ in certain complete families would lead to a proof of the effective Mordell conjecture, see [Pa, Vo, MB]. Unfortunately, such bounds seem out of reach. We summarize the known results in this direction. Javanpeykar [Ja] has given polynomial upper bounds in terms of the Belyi degree of X . While no bounds in complete families are known to date, there are some results for discrete families. Namely, for certain positive integers N , there are bounds for some modular curves, e.g. $X_0(N)$, $X_1(N)$ or $X(N)$, see [AU, MU, Kü2, Cu, May]. Upper bounds for minimal regular models of Fermat curves F_p of prime exponent p over $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p -th root of unity, were first computed in [Kü2] and vastly improved in [CK]. They were complemented by lower bounds in [KM, §6].

Building on our explicit description of \mathfrak{F}_N^{\min} from Part I of this work, we use a result due to Kühn [Kü2], which can be viewed as an Arakelov-theoretic Hurwitz formula on arithmetic surfaces, to compute upper bounds for $\bar{\omega}_{\mathfrak{F}_N^{\min}}^2$, when N is odd, squarefree and composite. This is similar to the strategy used in the case of prime exponents [CK]. We deduce the following result from the more precise Theorem 7.7:

Theorem 1.1. *Let $N > 0$ be an odd squarefree integer with at least two prime factors, and let \mathfrak{F}_N^{\min} be the minimal regular model of the Fermat curve F_N over $\mathbb{Z}[\zeta_N]$. Then the arithmetic self-intersection number of its dualizing sheaf over $\mathbb{Z}[\zeta_N]$, equipped with the Arakelov metric, satisfies*

$$(1.2) \quad \bar{\omega}_{\mathfrak{F}_N^{\min}}^2 \leq (2g - 2)\kappa\varphi(N) \log N + \mathcal{O}(g\varphi(N) \log \log N)$$

where $g = (N - 1)(N - 2)/2$ is the genus of F_N and $\kappa \in \mathbb{R}$ is a positive constant independent of N .

In other words, Theorem 1.1 yields an upper bound of order $N^2\varphi(N) \log N$. To complement Theorem 1.1, we also compute a lower bound for $\bar{\omega}_{\mathfrak{F}_N^{\min}}^2$ using the results of [KM]. These were already employed in [KM] in the case of prime exponents. The following explicit lower bound follows from Theorem 7.10:

Theorem 1.2. *In the notation of Theorem 1.1 we have the lower bound*

$$\bar{\omega}_{\mathfrak{F}_N^{\min}}^2 > \frac{1}{5N^2}\varphi(N) \log(N).$$

Although the results we obtain in Part II are Arakelov-theoretic, we treat the results from [Kü2] and [KM] as black boxes. This reduces the computation of our bounds to explicit computations of finite vertical intersection multiplicities on \mathfrak{F}_N^{\min} .

The paper is organized as follows: In Part I, we first recall some preliminary results from algebraic geometry in Section 2. These results are then used in Section 3 to construct the local minimal regular model $\mathfrak{F}_{N,\mathfrak{p}}^{\min}$ of F_N at a prime \mathfrak{p} of $\mathbb{Z}[\zeta_N]$ dividing N . We switch to a global perspective in Section 4 and construct the global minimal regular model \mathfrak{F}_N^{\min} of F_N over $\mathbb{Z}[\zeta_N]$.

Part II starts with a brief introduction to the arithmetic self intersection of the relative dualizing sheaf on an arithmetic surface and how to compute lower and upper bounds on it, see Section 5. In Section 6 we again work over a fixed prime \mathfrak{p} dividing N ; there we first study the extension of cusps of F_N with respect to the Belyi morphism $\beta : F_N \rightarrow \mathbb{P}^1$ given by $(X : Y : Z) \mapsto (X^N : Y^N)$. After that, we define certain vertical \mathbb{Q} -divisors on the local minimal regular model $\mathfrak{F}_{N,\mathfrak{p}}^{\min}$ and study their intersection properties. Finally we prove Theorem 1.1 and Theorem 1.2 in Section 7. The proofs crucially rely on the local results of Section 6.2.

The results of Sections 2, 3, 4, and of §6.1 and §7.1 also appear in the first author's PhD thesis [Cu], though the presentation has been shortened and some of the proofs given there are different from those presented here.

We would like to thank Ulf Kühn for suggesting the work described in the present paper and for answering many questions along the way. We are also grateful to Vincenz Busch, Ariyan Javanpeykar, Franz Király and Stefan Wewers for helpful discussions.

PART I: THE MINIMAL REGULAR MODEL OF FERMAT CURVES OF ODD SQUAREFREE EXPONENT

2. PRELIMINARIES

In the first two paragraphs we state a few results about regularity of Noetherian schemes and about explicit blow-ups. These will be used in Section 3 to construct the minimal regular model of the Fermat curve of odd squarefree exponent N over $\mathbb{Z}[\zeta_N]$. Although most of the results are well-known, some of the statements or proofs seem to be not easily accessible in the literature. We hope that it will be useful for the other applications to have these tools gathered in one place. The final paragraph contains relevant definitions and results on arithmetic surfaces.

2.1. Regularity. We first develop some tools that help to decide whether a given scheme or ring is regular.

Let A be a Noetherian local ring with maximal ideal \mathfrak{m} and residue class field $k(\mathfrak{m})$. Recall that A is *regular* if $\dim A = \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$. Alternatively, A is regular if and only if \mathfrak{m} can be generated by $\dim A$ elements.

More generally, let A be a Noetherian ring. If $\mathfrak{p} \subset A$ is a prime ideal, then we say that A is *regular at \mathfrak{p}* if the localization $A_{\mathfrak{p}}$ is a regular local ring. We say that A is *regular* if it is regular at each prime ideal.

Lemma 2.1. *Let A be a Noetherian ring and $\mathfrak{p} \subset A$ a prime ideal. Then A is regular at \mathfrak{p} if and only if $\mathfrak{p}A_{\mathfrak{p}}$ is generated by $\text{ht}(\mathfrak{p})$ elements.*

Proof: This is obvious, since $\text{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}}$. □

Lemma 2.2. *Let A be a regular Noetherian ring and S a multiplicative subset of A . Then A_S is regular.*

Proof: Let \mathfrak{P} be a prime ideal of A_S . This ideal is of the form $\mathfrak{p}A_S$, where \mathfrak{p} is a prime ideal of A disjoint from S , see e.g. [Mat, Theorem 4.1]. We have $(A_S)_{\mathfrak{p}A_S} = A_{\mathfrak{p}}$ by [Mat, Corollary 4.4], hence the regularity of A_S at \mathfrak{P} follows from the regularity of A at \mathfrak{p} . □

Lemma 2.3. *Let A be a Noetherian ring. Then A is regular if and only if it is regular at its maximal ideals.*

Proof: Follows from [Mat, Corollary 4.4]. □

In Section 3 we have to check the regularity of a factor ring A/f , where A is a regular ring and f is an element of A .

Lemma 2.4. *Let A/f be a factor ring, where A is a regular ring and f is an element of A . Furthermore, let \mathfrak{P} be a prime ideal of A/f and $\mathfrak{p} = \pi^{-1}\mathfrak{P}$, where $\pi : A \rightarrow A/f$ is the canonical surjection. Then A/f is regular at \mathfrak{P} if and only if $f \notin (\mathfrak{p}A_{\mathfrak{p}})^2$.*

Proof: The statement follows from [Liu, Corollary 4.2.12] and [Mat, Theorem 4.2]. \square

Let X be a locally Noetherian scheme and $x \in X$ a point. We say that X is *regular at x* if the stalk $\mathcal{O}_{X,x}$ at x of the structure sheaf \mathcal{O}_X is a regular local ring. We say that X is *regular* if it is regular at all of its points. If x is a point of X which is not regular we call it a *singular point of X* . A scheme that is not regular is said to be *singular*.

When our scheme comes with a flat morphism we can use the following useful result:

Lemma 2.5. *Let X and Y be locally Noetherian schemes and $g : X \rightarrow Y$ a flat morphism. If Y is regular at $y \in g(X)$, and $X_y = X \times_Y \operatorname{Spec} k(y)$ is regular at a point x , then X is regular at x .*

Proof: See [Gro, Corollaire 6.5.2]. \square

In the situations we consider later the scheme Y is already regular and we only need to take care of the scheme X_y . This scheme is a variety over the field $k(y)$. To analyze the points of this variety we can use the Jacobian criterion [Liu, Theorem 2.19].

Remark 2.6. Let us assume the morphism g in Lemma 2.5 is *faithfully flat*, i.e. flat and surjective. If Y and X_y are regular for all $y \in Y$ then X is regular. If X is regular then Y is regular by [Gro, Corollaire 6.5.2]. If Y is regular at y and X_y is singular at some x it may still happen that X is regular at x .

Now we are going to describe how we can use regularity to show normality.

Proposition 2.7. *Let R be a regular integral Noetherian ring and $f \in R \setminus R^*$. If R/f is regular in codimension 1, then R/f is normal.*

Proof: Since R is a regular ring, it is a Cohen-Macaulay ring. We want to show that R/f is a Cohen-Macaulay ring as well. Let $\mathfrak{m} \in \operatorname{Max}(R/f)$ and $\mathfrak{M} \in \operatorname{Max}(R)$ be the preimage of \mathfrak{m} . Since localization commutes with passing to quotients by ideals, we have

$$(R/f)_{\mathfrak{m}} = R_{\mathfrak{M}}/fR_{\mathfrak{M}}.$$

Now f is a regular element of $R_{\mathfrak{M}}$ and so $R_{\mathfrak{M}}/fR_{\mathfrak{M}}$ is a Cohen-Macaulay ring (see [Liu, Proposition 8.2.15]). Because our computation is valid for all maximal ideals of R/f , the ring R/f is Cohen-Macaulay, cf. [Ei, Proposition 18.8]. The statement follows using Serre's criterion, see for instance [Liu, Theorem 8.2.23]. \square

2.2. Blow-ups. In the study of birational morphisms blow-ups play an important role. We summarize the main facts we need about them. Most of the material we introduce is standard and the proofs may be found, for instance, in [Liu] and [EH]. Later we will prove a result which deals with the concrete situation that we will encounter in Section 3. Apart from this we mostly follow Liu's book [Liu].

To start with, let A be a Noetherian ring and I an ideal of A . We denote by \tilde{A} the graded A -algebra

$$\tilde{A} = \bigoplus_{d \geq 0} I^d, \text{ where } I^0 := A.$$

Definition 2.8. Let $X = \operatorname{Spec} A$ be an affine Noetherian scheme, I an ideal of A , and $\tilde{X} = \operatorname{Proj} \tilde{A}$. The scheme \tilde{X} together with the canonical morphism $\tilde{X} \rightarrow X$ is called the *blow-up of X along $V(I)$* .

The blow-up has the following properties.

Lemma 2.9. *Let A be a Noetherian ring, and let I be an ideal of A .*

- (1) *The ring \tilde{A} is integral if and only if A is integral.*
- (2) *Let B be a flat A -algebra, and let \tilde{B} be the graded B -algebra associated to the ideal IB . Then we have a canonical isomorphism $\tilde{B} \cong B \otimes_A \tilde{A}$.*

Proof: See [Liu, Lemma 8.1.2]. □

Now let $I = (a_1, \dots, a_r)$. We denote by $t_i \in I = \tilde{A}_1$ the element a_i , considered as a homogeneous element of degree 1. We have a surjective homomorphism of graded A -algebras

$$\phi : A[X_1, \dots, X_r] \rightarrow \tilde{A}$$

defined by $\phi(X_i) = t_i$. It follows that \tilde{A} is isomorphic to a factor ring $A[X_1, \dots, X_r]/J$; here J denotes an ideal of $A[X_1, \dots, X_r]$. It may be desirable for certain applications to express the blow-up in such a way. Unfortunately it is not always easy to describe the ideal J explicitly. However, if the ideal I is generated by a regular sequence, we have a simple description of J .

Lemma 2.10. *Let $I \subset A$ be an ideal which is generated by a regular sequence a_1, \dots, a_r . Then $\tilde{A} \cong A[X_1, \dots, X_r]/J$ where the ideal J is generated by the elements of the form $X_i a_j - X_j a_i$ for $1 \leq i, j \leq r$.*

Proof: See [EH, Proposition IV-25, Exercise IV-26]. □

Later on, we will mostly work with integral rings. Here we have the following situation:

Lemma 2.11. *Let A be a Noetherian integral ring and $I = (a_1, \dots, a_r)$ an ideal of A such that $a_i \neq 0$ for all i . The blow-up $\tilde{X} \rightarrow X = \operatorname{Spec} A$ along $V(I)$ is the union of the affine open subschemes $\operatorname{Spec} A_i$, $1 \leq i \leq r$, where A_i is the sub- A -algebra*

$$A\left[\frac{a_1}{a_i}, \dots, \frac{a_r}{a_i}\right]$$

of the field $\operatorname{Frac}(A)$ generated by the $\frac{a_j}{a_i} \in \operatorname{Frac}(A)$, $1 \leq j \leq r$.

Proof: See for instance [Liu, Lemma 8.1.4]. □

Lemma 2.12. *Let A be an integral Noetherian ring, a_1, \dots, a_r a regular sequence, and $I = (a_1, \dots, a_r)$. We have:*

- (1) *The ring*

$$R = A[X_1, \dots, \widehat{X_i}, \dots, X_r]/J$$

is integral, where J is generated by the elements $a_j - X_j a_i$ with $1 \leq j \leq r$ and $j \neq i$.

- (2) *For an element $f \in A$ let \bar{f} denote its image in R . We have*

$$f \in I^d \Leftrightarrow \bar{f} \in (\bar{a_i})^d.$$

Proof: Since A is integral, \tilde{A} is integral as well by Lemma 2.9. We know that

$$\tilde{A} \cong A[X_1, \dots, X_r]/J,$$

where J is generated by the elements $X_i a_j - X_j a_i$ for $1 \leq i, j \leq r$, see Lemma 2.10. Hence $\text{Spec } R$ is an affine open subset of $\text{Proj } \tilde{A}$ and therefore integral. This proves the first statement.

For the second statement we assume $i = 1$ for simplicity. Let $f \in I^d$. Then there exists a homogeneous polynomial $F(X) = F(X_1, \dots, X_r) \in A[X_1, \dots, X_r]$ of degree d such that $f = F(a) = F(a_1, \dots, a_r)$. If we set

$$f_0 = \frac{F(a_1, X_2 a_1, \dots, X_r a_1)}{a_1^d} = F(1, X_2, \dots, X_r),$$

then we obviously have $\bar{f} = \bar{f}_0 \bar{a}_1^d$ and therefore $\bar{f} \in (\bar{a}_1)^d$.

Now let $\bar{f} \in (\bar{a}_1)^d$. Furthermore, let n be the largest integer such that $f \in I^n$. Let us assume $n < d$. As above, there is a homogeneous polynomial $F(X)$ of degree n with $F(a) = f$. It follows that not all coefficients of $F(X)$ are in I because otherwise we would have $f \in I^{n+1}$. Now $f_0 = \frac{F(a_1, X_2 a_1, \dots, X_r a_1)}{a_1^n}$ is a polynomial in X_2, \dots, X_r whose coefficients are not all in I . We have $\bar{f} = \bar{f}_0 \bar{a}_1^n$, but, since R is integral and $\bar{f} \in (\bar{a}_1)^d$ with $n < d$, the element \bar{a}_1 must divide \bar{f}_0 . Therefore $f_0 = a_1 G(X) + H(X)$, where $G(X) \in A[X_2, \dots, X_r]$ and $H(X) \in J$. It follows that all coefficients of f_0 are in I , a contradiction. In other words, we have $d \leq n$ and therefore $f \in I^d$. \square

So far we have discussed the blow-up of an integral scheme along a subscheme associated to an ideal generated by a regular sequence. Unfortunately, we will encounter more involved blow-ups in Section 3. However, in those situations the following theorem will come to our aid.

Theorem 2.13. *Let A be an integral Noetherian ring, a_1, \dots, a_r a regular sequence, and $I = (a_1, \dots, a_r)$ a prime ideal of A . Furthermore, let $f \in I$ and n be the largest integer such that $f \in I^n$. Then*

$$A[X_1, \dots, \widehat{X_i}, \dots, X_r]/J_0 \cong A/f[\frac{a_1}{a_i}, \dots, \frac{a_r}{a_i}],$$

where J_0 is the ideal generated by the $a_j - X_j a_i$ (with $1 \leq j \leq r$ and $j \neq i$) and a polynomial f_0 such that $f \equiv f_0 a_i^n \pmod{J}$; here \mathbf{a}_j denotes the residue class of a_j in A/f and J is the ideal from Lemma 2.12.

Proof: For simplicity we assume $i = 1$. The canonical surjection

$$\begin{aligned} \varphi : A[X_2, \dots, X_r] &\longrightarrow A/f[\frac{a_2}{a_1}, \dots, \frac{a_r}{a_1}] \\ F(X_2, \dots, X_r) &\longmapsto \mathbf{F}(\frac{a_2}{a_1}, \dots, \frac{a_r}{a_1}) \end{aligned}$$

(here the bold \mathbf{F} indicates that we reduce the coefficients of the polynomial modulo f) induces, since $a_i - X_i a_1 \in \ker \varphi$, a surjection

$$\begin{aligned} \phi : A[X_2, \dots, X_r]/J &\longrightarrow A/f[\frac{a_2}{a_1}, \dots, \frac{a_r}{a_1}] \\ \overline{F}(\overline{X_2}, \dots, \overline{X_r}) &\longmapsto \mathbf{F}(\frac{a_2}{a_1}, \dots, \frac{a_r}{a_1}), \end{aligned}$$

where J is the ideal from Lemma 2.12. We get the following commutative diagram

$$(2.1) \quad \begin{array}{ccc} A[X_2, \dots, X_r]/J & \xrightarrow{\phi} & A/f[\frac{a_2}{a_1}, \dots, \frac{a_r}{a_1}] \\ \uparrow & & \uparrow \\ A & \xrightarrow{\pi} & A/f \end{array}$$

Next we want to investigate the kernel of the map ϕ . Let $x = \overline{F(\overline{X}_2, \dots, \overline{X}_r)}$, where $F(X_2, \dots, X_r)$ is a polynomial of degree m and $\phi(x) = 0$. We have $a_1^m F(X_2, \dots, X_r) \equiv \mu \pmod{J}$, where $\mu \in A$. Since diagram (2.1) is commutative and the right arrow in this diagram is injective, we have $\pi(\mu) = 0$. It follows that $\mu = \lambda f$ for some $\lambda \in A$. Now let n (n_λ resp.) be the largest integer such that $f \in I^n$ ($\lambda \in I^{n_\lambda}$ resp.) and $f_0 \in A[X_2, \dots, X_r]$ ($\lambda_0 \in A[X_2, \dots, X_r]$ resp.) with $\overline{a_1^n f_0} = \overline{f}$ ($\overline{a_1^{n_\lambda} \lambda_0} = \overline{\lambda}$ resp.). We have

$$(2.2) \quad \overline{a_1^m x} = \overline{f \lambda} = \overline{a_1^n f_0 a_1^{n_\lambda} \lambda_0}$$

in $A[X_2, \dots, X_r]/J$. If we assume that $m \leq n + n_\lambda$, then we can cancel $\overline{a_1^m}$ in equation (2.2) by Lemma 2.12 and it follows that x is in the ideal $(\overline{f_0})$. So if we can show that $m > n + n_\lambda$ is impossible, then we are done. According to (2.2) we have $\lambda f \in I^m$ by Lemma 2.12. Now $m > n + n_\lambda$ would imply that the associated graded algebra $\text{gr}_I(A)$ is not integral. But a_1, \dots, a_r is a regular sequence and so we have an A/I -algebra isomorphism

$$\text{Sym}(I/I^2) \cong \text{gr}_I(A)$$

(see [Hu]) where $\text{Sym}(I/I^2)$ is integral, because I is a prime ideal. This finishes the proof by contradiction. \square

Remark 2.14. The schemes we have to consider later are of the form $\text{Spec } A/f$ (at least locally), where A is a ring and $f \in A$ is a prime element. The blow-up of A/f along $V(I/f)$ is covered by the spectra of the rings

$$A/f[\frac{a_1}{a_i}, \dots, \frac{a_r}{a_i}],$$

where a_j is the residue class of a_j in A/f and $I = (a_1, \dots, a_r)$, cf. Lemma 2.11. According to Theorem 2.13 we can express these rings explicitly as factor rings if the a_j form a regular sequence and I is a prime ideal. To do this, we only need to know the largest integer n such that $f \in I^n$ and polynomials $f_{0,i}$ such that $f \equiv f_{0,i} a_i^n \pmod{J}$. We can use the following strategy to find these quantities: We only need to find a homogeneous polynomial $F(X) \in A[X_1, \dots, X_r]$ such that not all coefficients are in I and such that $F(a) = f$. Obviously $f \in I^n$, where n is the degree of $F(X)$. Because a_1, \dots, a_r is a regular sequence, it is a quasi-regular sequence as well, see [Mat, Theorem 16.2]. It follows that if $f \in I^{n+1}$, then all coefficients of $F(X)$ are in I , a contradiction. So n is the largest integer such that $f \in I^n$. We can compute the $f_{0,i}$ as in the proof of Lemma 2.12. More precisely, we have

$$f_{0,i} = F(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_r).$$

We briefly describe how to extend the construction of blow-ups of affine scheme to arbitrary schemes. In this situation we need to use a coherent sheaf of ideals to construct the blow-up.

Definition 2.15. Let X be a Noetherian scheme, and \mathcal{I} be a coherent sheaf of ideals on X . Consider the sheaf of graded algebras $\bigoplus_{d \geq 0} \mathcal{I}^d$, where \mathcal{I}^d is the d -th power of the ideal \mathcal{I} , and set $\mathcal{I}^0 = \mathcal{O}_X$. Then $\widetilde{X} = \text{Proj } \bigoplus_{d \geq 0} \mathcal{I}^d$ is the *blow-up of X with respect*

to \mathcal{I} . If Y is the closed subscheme of X corresponding to \mathcal{I} , then we also call \tilde{X} the *blow-up of X along Y* .

Proposition 2.16. *Let X be a locally Noetherian scheme, and let \mathcal{I} be a coherent sheaf of ideals on X . Let $\pi : \tilde{X} \rightarrow X$ be the blow-up of X along $Y = V(\mathcal{I})$. Then we have the following properties:*

- (1) *The morphism π is proper.*
- (2) *Let $Z \rightarrow X$ be a flat morphism with Z locally Noetherian. Let $\tilde{Z} \rightarrow Z$ be the blow-up of Z along $\mathcal{I}\mathcal{O}_Z$; then $\tilde{Z} \cong \tilde{X} \times_X Z$.*
- (3) *The morphism π induces an isomorphism $\pi^{-1}(X \setminus V(\mathcal{I})) \rightarrow X \setminus V(\mathcal{I})$. If X is integral, and if $\mathcal{I} \neq 0$, then \tilde{X} is integral, and π is a birational morphism.*

Proof: See for instance [Liu, Proposition 8.1.12]. □

Now let us assume that X is a locally Noetherian scheme that comes with a closed immersion $f : X \rightarrow Z$ to a locally Noetherian scheme Z . Let \mathcal{J} be a quasi-coherent sheaf of ideals on Z with the property that $f(X)$ is not contained in the center $V(\mathcal{J})$. Then the blow-up \tilde{X} of X along \mathcal{I} , where $\mathcal{I} = (f^{-1}\mathcal{J})\mathcal{O}_X$, is a closed immersion of the blow-up \tilde{Z} of Z along \mathcal{J} , see for instance [Liu, Corollary 1.16]. The closed subscheme $\tilde{X} \subseteq \tilde{Z}$ is called the *strict transform* of X . In our applications the scheme X will be a singular scheme which is a subscheme of a regular scheme Z . We will use a sequence of blow-ups of X to compute a desingularization of this scheme. Each of these blow-ups comes from a blow-up of the scheme Z . The blow-ups of Z are regular by [Liu, Theorem 8.1.19].

2.3. Intersection theory on arithmetic surfaces. Let R be a Dedekind ring with field of fractions K . If $\pi : \mathcal{X} \rightarrow \operatorname{Spec} R$ is a projective flat morphism and \mathcal{X} a regular integral scheme of dimension 2 such that the generic fiber

$$\mathcal{X}_K = \mathcal{X} \times_{\operatorname{Spec} R} \operatorname{Spec} K$$

of π is geometrically irreducible, we call \mathcal{X} an *arithmetic surface*. If X/K is a geometrically irreducible smooth projective curve and \mathcal{X} is an arithmetic surface over R whose generic fiber \mathcal{X}_K is isomorphic to X , then we call \mathcal{X} a *(projective) regular model* of X over R . Such a model always exists, see for instance [Lip2]. Moreover, if the genus of X is at least 1, then there always exists a regular model \mathcal{X}^{\min} of X over R , unique up to isomorphism, such that every R -birational morphism $\mathcal{X}^{\min} \rightarrow \mathcal{X}$ to another regular model \mathcal{X} of X over R is an isomorphism. We call \mathcal{X}^{\min} the *minimal regular model* of X over R . A regular model \mathcal{X} of X over R is minimal if and only if none of its irreducible components can be contracted by a blow-up morphism such that the resulting model remains regular; such components are called *exceptional*. If \mathcal{C} is a component of a special fiber \mathcal{X}_s that is defined over an algebraically closed field, then, by Castelnuovo's criterion [Liu, Theorem 9.3.8], \mathcal{C} is exceptional if and only if it has genus 0 and self-intersection -1 , see below.

Let $\pi : \mathcal{X} \rightarrow \operatorname{Spec} R$ be an arithmetic surface. If $s \in \operatorname{Spec} R$ is a closed point and D, E are divisors on \mathcal{X} without common component, we denote by $(D \cdot E)_s$ the rational-valued intersection multiplicity between D and E (cf. [Liu, §9.1.2]); we simply write $(D \cdot E)$ if it is clear which s we are working over. If D is a vertical divisor on \mathcal{X} with support in the fiber \mathcal{X}_s , then we can use the moving lemma [Liu, Corollary 9.1.10] to define the self-intersection D_s^2 (or D^2). We extend the intersection multiplicity (\cdot) to the group

$$\operatorname{Div}(\mathcal{X})_{\mathbb{Q}} := \operatorname{Div}(\mathcal{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$$

of \mathbb{Q} -divisors on \mathcal{X} by linearity.

Let $\omega_{\mathcal{X}/R}$ denote the *relative dualizing sheaf* of \mathcal{X} over R . We call a divisor \mathcal{K} of \mathcal{X} such that $\mathcal{O}_{\mathcal{X}}(\mathcal{K}) \cong \omega_{\mathcal{X}/R}$ a *canonical divisor*. More generally, we call a divisor $\mathcal{K} \in \text{Div}(\mathcal{X})_{\mathbb{Q}}$ such that $\mathcal{O}_{\mathcal{X}}(\mathcal{K}) \cong \omega_{\mathcal{X}/R}$ in $\text{Pic}(\mathcal{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$ a *canonical \mathbb{Q} -divisor*. If \mathcal{E} is an effective nonzero vertical divisor, we define

$$(2.3) \quad a_{\mathcal{E}} := \mathcal{E}^2 - 2p_a(\mathcal{E}) + 2.$$

where $p_a(\mathcal{E})$ is the arithmetic genus of \mathcal{E} .

Theorem 2.17 (Adjunction formula). *Let \mathcal{K} be a canonical \mathbb{Q} -divisor on \mathcal{X} and let $\mathcal{E} \neq 0$ be an effective vertical divisor on \mathcal{X} . Then we have*

$$(2.4) \quad a_{\mathcal{E}} = (\mathcal{K} \cdot \mathcal{E}).$$

Proof: See [Liu, Theorem 8.1.37] for the case $\mathcal{K} \in \text{Div}(\mathcal{X})$. The extension to $\mathcal{K} \in \text{Div}(\mathcal{X})_{\mathbb{Q}}$ is immediate. \square

We will use the adjunction formula extensively, especially in Section 6.2.

3. THE LOCAL MINIMAL REGULAR MODEL

Let N be an odd squarefree natural number which is not prime and let ζ_N be a primitive N -th root of unity. Recall that the Fermat curve $F_N/\mathbb{Q}(\zeta_N)$ is defined by

$$F_N : X^N + Y^N = Z^N.$$

Let p be a prime number such that $N = pm$ with $m \in \mathbb{N}$ and fix a prime ideal \mathfrak{p} of $\mathbb{Z}[\zeta_N]$ that lies above p . We denote by R the localization of $\mathbb{Z}[\zeta_N]$ with respect to \mathfrak{p} . In this section we construct the minimal regular model of $F_N \times_{\text{Spec } \mathbb{Z}[\zeta_N]} \text{Spec } R$, see Theorem 3.13.

Let π be a uniformizing element of R and let $k(\pi)$ denote its residue field, viewed as a subfield of $\overline{\mathbb{F}}_p$. We can and will also interpret this element as a uniformizing element of the strict Henselization R^{sh} . Consider the model

$$\mathfrak{F}_{N,\mathfrak{p}}^0 = \text{Proj } R[X, Y, Z]/(X^N + Y^N - Z^N).$$

To construct the minimal regular model of $F_N \times_{\text{Spec } \mathbb{Z}[\zeta_N]} \text{Spec } R$ we work with affine open subschemes of $\mathfrak{F}_{N,\mathfrak{p}}^0$. In particular, we consider the integral affine open subscheme

$$(3.1) \quad \mathcal{X} := \text{Spec } R[X, Y]/(X^N + Y^N - 1)$$

of $\mathfrak{F}_{N,\mathfrak{p}}^0$. For a natural number n we will also use F_n to denote the polynomial $X^n + Y^n - 1$. It will be clear from the context whether we refer to the Fermat curve or to the polynomial, by abuse of notation. For the following computations it will be useful to rewrite $X^N + Y^N - 1$ as

$$(3.2) \quad F_m^p + p\psi(X^m, Y^m),$$

where

$$(3.3) \quad \psi(a, b) = \frac{a^p + b^p - 1 - (a + b - 1)^p}{p}.$$

Note that there is a unit μ of R such that $p = \mu\pi^{p-1}$. Using (3.2), it can be seen easily that the special fiber of \mathcal{X} is of the form

$$\text{Spec}(R[X, Y]/(F_m^p + p\psi(X^m, Y^m)) \otimes_R k(\pi)) = \text{Spec}(k(\pi)[X, Y]/F_m^p).$$

Therefore the special fiber consists of a single component \mathcal{C} , which has multiplicity p . This component – considered as a subset of \mathcal{X} – is the closure of the ideal $I = (\pi, F_m) \subset R[X, Y]/(X^N + Y^N - 1)$, so $V(I) = \mathcal{C}$. The ideal I is a prime ideal, as the ring

$$R[X, Y]/I \cong k(\pi)[X, Y]/(X^m + Y^m - 1)$$

is integral. Because of the regularity of this ring, the closed subscheme \mathcal{C} is regular. However, since $F_N \in I^{p-1}$ and $p \neq 2$, the scheme \mathcal{X} is singular. In fact, it is not even normal, because it is not regular in codimension 1.

3.1. The polynomial $\psi(X^m, Y^m)$. In this paragraph we are going to study the polynomial $\psi(X^m, Y^m)$, see (3.3). In order to do this we analyze the polynomial $\psi(a, b)$ and then evaluate it in X^m and Y^m later on. We have the following:

$$\begin{aligned} \psi(a, b) - \psi(a, 1 - a) &= \frac{a^p + b^p - 1 - (a + b - 1)^p}{p} - \frac{a^p + (1 - a)^p - 1}{p} \\ &= \frac{b^p - (a + b - 1)^p + (a - 1)^p}{p} \\ &= \sum_{k=1}^{p-1} \frac{\binom{p}{k}}{p} (a + b - 1)^{p-k} b^k (-1)^k. \end{aligned}$$

Substituting X^m for a and Y^m for b we get

$$(3.4) \quad \psi(X^m, Y^m) = \psi(X^m, 1 - X^m) + \sum_{k=1}^{p-1} \frac{\binom{p}{k}}{p} F_m^{p-k} Y^{mk} (-1)^k$$

For later computations it will be important to know the factorization of $\psi(X^m, Y^m)$ into irreducibles. We first recall a result of McCallum [Mc].

Lemma 3.1. *There is a decomposition*

$$(3.5) \quad \psi(a, 1 - a) = a(a - 1)\Psi(a),$$

with a polynomial $\Psi(a) \in R[a]$. In the prime factorization of $\Psi(a)$ over $\overline{\mathbb{F}}_p$, factors occur with multiplicity one if they are not rational over \mathbb{F}_p , and with multiplicity two otherwise.

Proof: We elaborate on the proof of the Lemma on page 59 of [Mc]. We have $(\psi(a, 1 - a))' = a^{p-1} - (1 - a)^{p-1} \equiv -(a - 2) \cdots (a - p + 1) \pmod{\pi}$. The only roots of $\psi(a, 1 - a) \pmod{\pi}$ with multiplicity greater than one are of the form $\bar{\alpha} \in \{2, \dots, \overline{p-1}\}$ with $\alpha \in R$. If the multiplicity of $\bar{\alpha}$ were greater than two, then the second derivative would vanish in $\bar{\alpha}$ as well. But from $(p - 1)\alpha^{p-2} + (p - 1)(1 - \alpha)^{p-2} \equiv 0 \pmod{\pi}$ it follows that $\alpha^{p-2} \equiv (\alpha - 1)^{p-2} \pmod{\pi}$, so by multiplication with $\alpha(\alpha - 1)$ we obtain $\alpha - 1 \equiv \alpha \pmod{\pi}$ and this is obviously impossible. Let us denote the root of multiplicity 2 by $\bar{\alpha}_1, \dots, \bar{\alpha}_s$

Together with the fact that 0 and 1 are simple roots of $\psi(a, 1 - a)$ and $\bar{\psi}(a, 1 - a)$, we get the decomposition

$$(3.6) \quad \bar{\psi}(a, 1 - a) = a(a - 1)(a - \bar{\beta}_1) \cdots (a - \bar{\beta}_r)(a - \bar{\alpha}_1)^2 \cdots (a - \bar{\alpha}_s)^2,$$

over $\overline{\mathbb{F}}_p$, where $\bar{\beta}_i \notin \mathbb{F}_p$. with some irreducible polynomials $\bar{f}_i(a)$. Since in this decomposition all factors are pairwise coprime and $\deg \psi(a, 1 - a) = \deg \bar{\psi}(a, 1 - a)$, the claim follows from Hensel's lemma. \square

Corollary 3.2. *There is a decomposition*

$$(3.7) \quad \psi(X^m, 1 - X^m) = X^m \prod_{i=0}^{m-1} (X - \zeta_m^i) \Psi(X^m).$$

In the prime factorization of $\Psi(X^m)$ over $\overline{\mathbb{F}}_p$, factors $(X - \bar{\delta})$ occur with multiplicity 1 if $\bar{\delta}^m$ is not rational over \mathbb{F}_p , and with multiplicity 2 otherwise.

Proof: If we replace a by X^m in (3.5), it is obvious that we get (3.7), since $\zeta_m^i \in R$. A decomposition as in (3.6) becomes

$$\bar{\psi}(X^m, 1 - X^m) = X^m \prod_{i=0}^{m-1} (X - \bar{\zeta}_m^i)(X - \bar{\delta}_1) \cdots (X - \bar{\delta}_{rm})(X - \bar{\gamma}_1)^2 \cdots (X - \bar{\gamma}_{sm})^2$$

after this substitution; here $\bar{\delta}^m = \bar{\beta}$ and $\bar{\gamma}^m = \bar{\alpha}$. Since the $\bar{\alpha}_i$ and $\bar{\beta}_j$ from Lemma 3.1 are non-zero, the polynomials $X^m - \bar{\alpha}_i$ and $X^m - \bar{\beta}_j$ split into coprime linear factors over $\overline{\mathbb{F}}_p$. The linear polynomials $(X - \bar{\gamma}_k)$ are the only factors of multiplicity two in $\Psi(X^m)$ over $\overline{\mathbb{F}}_p$. \square

Definition 3.3. Let us denote by ϱ the number of factors $(X - \bar{\gamma}_k)^2$ of $\Psi(X^m, 1 - X^m)$ over $\overline{\mathbb{F}}_p$.

Remark 3.4. As $\psi(a, 1 - a)$ is a polynomial of degree $p - 1$, the polynomial $\psi(X^m, 1 - X^m)$ is of degree $m(p - 1)$. Corollary 3.2 tells us that there are

$$\deg \Psi(X^m) - 2\varrho = m(p - 3) - 2\varrho$$

linear factors of multiplicity one in $\Psi(X^m)$. For instance, let $p = 5$. Then $\Psi_5(a) \equiv a^2 - a + 1 \pmod{5}$, where $a^2 - a + 1$ is an irreducible element of $\mathbb{F}_5[a]$. It follows that in this case $\varrho = 0$. On the other hand, consider the case $p = 7$. Here we have $\Psi_7(a) \equiv (a + 2)^2(a + 4)^2 \pmod{7}$, hence $\varrho = \frac{1}{2} \deg \Psi_7(X^m) = 2m$.

3.2. The blow-up of \mathcal{X} along $V(I)$. We start by giving an explicit description of the blow-up.

Proposition 3.5. *Let I denote the ideal $I = (\pi, F_m) \subset R[X, Y]/F_N$. Then the blow-up $\tilde{\mathcal{X}}$ of the scheme \mathcal{X} in (3.1) along $V(I)$ is given by the affine open subsets $U_1 = \text{Spec } S_1$ and $U_2 = \text{Spec } S_2$, where*

$$(3.8) \quad S_1 = R[X, Y, W_1]/(F_m - W_1\pi, \pi W_1^p + \mu\psi(X^m, Y^m))$$

and

$$(3.9) \quad S_2 = R[X, Y, W_2]/(W_2F_m - \pi, F_m + \mu W_2^{p-1}\psi(X^m, Y^m)).$$

In other words, we have $\tilde{\mathcal{X}} = U_1 \cup U_2$.

Proof: The generators of the ideal I obviously form a regular sequence in $R[X, Y]$, since $R[X, Y]$ and $R[X, Y]/\pi$ ($R[X, Y]/F_m$ resp.) are integral. Therefore we can apply Theorem 2.13. The polynomial

$$F_m W_1^{p-1} + \mu W_2^{p-1} \psi(X^m, Y^m) \in (R[X, Y])[W_1, W_2]$$

is homogeneous in W_1 and W_2 and the coefficient $\mu\psi(X^m, Y^m)$ is not in the ideal I . The statement follows now with Remark 2.14. \square

Remark 3.6. The scheme $\tilde{\mathcal{X}}$ can be considered as a subscheme of the scheme $\tilde{\mathcal{Z}} = V_1 \cup V_2$, where

$$V_1 = \operatorname{Spec} R[X, Y, W_1]/(F_m - W_1\pi)$$

and

$$V_2 = \operatorname{Spec} R[X, Y, W_2]/(W_2F_m - \pi).$$

Since $\tilde{\mathcal{Z}}$ is just the blow-up of the regular scheme $\mathcal{Z} = \operatorname{Spec} R[X, Y]$ along (π, F_m) , it is regular as well by [Liu, Lemma 8.1.4] and [Liu, Theorem 8.1.19]. The scheme $\tilde{\mathcal{X}}$ is the strict transform of \mathcal{X} in $\tilde{\mathcal{Z}}$.

Proposition 3.7. *The scheme $\tilde{\mathcal{X}}$ from Proposition 3.5 is normal. Let $\bar{F}_m, \bar{\psi}(X^m, 1 - X^m) \in \bar{\mathbb{F}}_p[X, Y]$ be the respective reductions of F_m and $\psi(X^m, 1 - X^m)$ with respect to the canonical morphism $R[X, Y] \rightarrow \bar{\mathbb{F}}_p[X, Y]$. The geometric special fiber $\tilde{\mathcal{X}} \times_{\operatorname{Spec} R} \operatorname{Spec} \bar{\mathbb{F}}_p$ has configuration as in Figure 1, where the components $L_{(x,y)}$ are of genus 0 and are parameterized by those pairs $(x, y) \in \bar{\mathbb{F}}_p^2$ which satisfy*

$$x^m + y^m - 1 = \bar{\psi}(x^m, 1 - x^m) = 0.$$

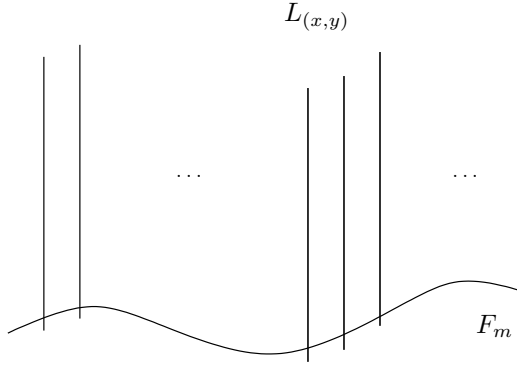


FIGURE 1. The configuration of the geometric special fiber $\tilde{\mathcal{X}} \times_{\operatorname{Spec} R} \operatorname{Spec} \bar{\mathbb{F}}_p$.

Proof: We work with the scheme

$$(3.10) \quad \tilde{\mathcal{X}}^{sh} = \tilde{\mathcal{X}} \times_{\operatorname{Spec} R} \operatorname{Spec} R^{sh}$$

whose special fiber is a variety over the algebraically closed field $\bar{\mathbb{F}}_p$. Since this base change is faithfully flat, normality of $\tilde{\mathcal{X}}^{sh}$ implies normality of $\tilde{\mathcal{X}}$. We start our computation with the affine open subscheme $U_1^{sh} = \operatorname{Spec} S_1^{sh}$, where $S_1^{sh} = S_1 \otimes_R R^{sh}$. The special fiber of this scheme is

$$(3.11) \quad \begin{aligned} U_1^{sh} \times_{\operatorname{Spec} R^{sh}} \operatorname{Spec} \bar{\mathbb{F}}_p &= \operatorname{Spec} (\bar{\mathbb{F}}_p[X, Y, W_1]/(F_m, \psi(X^m, Y^m))) \\ &= \operatorname{Spec} (\bar{\mathbb{F}}_p[X, Y, W_1]/(F_m, \psi(X^m, 1 - X^m))) . \end{aligned}$$

This variety consists of lines $L_{x,y} = V(X - x, Y - y)$, where x is a root of $\bar{\psi}(X^m, 1 - X^m)$ and y is a root of $Y^m + x^m - 1 \in \bar{\mathbb{F}}_p[Y]$. These lines correspond to prime divisors $V(\mathfrak{P})$ of U_1^{sh} , where $\mathfrak{P} = (X - X', Y - Y', \pi)$ is a prime ideal of height 1 and $X' \equiv x \pmod{\pi}$ ($Y' \equiv y \pmod{\pi}$ resp.). Because of Remark 3.6 and Proposition 2.7, it suffices to show that S_1^{sh} is regular at \mathfrak{P} (since the generic fiber of $\tilde{\mathcal{X}}^{sh}$ (U_1^{sh} resp.) is regular, S_1^{sh} is

regular at every prime ideal which does not contain π). Note that π cannot be a divisor of X' and of Y' , as $x^m + y^m = 1$. Because of symmetry, we may assume $\pi \nmid Y'$ without loss of generality. We have $\psi(X'^m, 1 - X'^m) = \lambda\pi$, where $\lambda \in R^{sh}$. Now,

$$\psi(X^m, 1 - X^m) = \lambda\pi + (X - X')G(X),$$

where $G(X) \in R^{sh}[X]$. It follows from Proposition 3.5 and equation (3.4) that

$$-(X - X')G(X) = \pi \left(W_1^p \mu^{-1} + W_1 Y^{m(p-1)} + \lambda + \pi H(Y, W_1) \right)$$

in S_1^{sh} , where $H(Y, W_1) \in R^{sh}[Y, W_1]$.

Let us suppose that $W_1^p \mu^{-1} + W_1 Y^{m(p-1)} + \lambda + \pi H(Y, W_1) \in \mathfrak{P}$. Then $W_1^p \mu^{-1} + W_1 Y^{m(p-1)} + \lambda \in \mathfrak{P}$ and (using Hensel's lemma) we have $(W_1 - W') \in \mathfrak{P}$, where W' is a root of $W_1^p \mu^{-1} + W_1 Y^{m(p-1)} + \lambda =: f(W_1) \in R^{sh}[W_1]$. Indeed, since $\bar{f}'(W_1) = y^{m(p-1)} \neq 0$ the polynomial $\bar{f}(W_1)$ splits into coprime linear factors in $\bar{\mathbb{F}}_p$, and this decomposition lifts to R^{sh} . But if this linear factor is in \mathfrak{P} , then \mathfrak{P} is a maximal ideal; a contradiction, because \mathfrak{P} was assumed to be of height 1. Hence we have

$$W_1^p \mu^{-1} + W_1 Y^{m(p-1)} + \lambda + \pi H(Y, W_1) \notin \mathfrak{P},$$

and so this element becomes a unit in $(S_1^{sh})_{\mathfrak{P}}$. We denote this unit by ϵ .

Note that, since $\pi | X'^m + Y'^m - 1$, we have $X'^m + Y'^m - 1 = \tau\pi$, where $\tau \in R^{sh}$. Using Proposition 3.5, it follows that

$$\begin{aligned} \pi W_1 &= X^m + Y^m - 1 \\ &= X^m - X'^m + Y^m - Y'^m + X'^m + Y'^m - 1 \\ &= (X - X') \prod_{i=1}^{m-1} (X - X' \zeta_m^i) + (Y - Y') \prod_{i=1}^{m-1} (Y - Y' \zeta_m^i) + \tau\pi \end{aligned}$$

in S_1^{sh} . Now, $\prod_{i=1}^{m-1} (Y - Y' \zeta_m^i) \notin \mathfrak{P}$ because otherwise $Y' \in \mathfrak{P}$ or $(1 - \zeta_m^i) \in \mathfrak{P}$ and this is impossible, since these elements are units in R^{sh} . To see this, recall that $\pi \nmid Y'$, and that $(1 - \zeta_m^i)$ is a divisor of m and m is coprime to p . Therefore $\prod_{i=1}^{m-1} (Y - Y' \zeta_m^i)$ is a unit in $(S_1^{sh})_{\mathfrak{P}}$. We will denote this unit by ϵ' . In the localization $(S_1^{sh})_{\mathfrak{P}}$ we have

$$-(X - X')G(X) \frac{1}{\epsilon} = \pi$$

and

$$-(X - X') \left(\prod_{i=1}^{m-1} (X - X' \zeta_m^i) + G(X) \frac{1}{\epsilon} (W_1 - \tau) \right) \frac{1}{\epsilon'} = (Y - Y').$$

Hence we have $\mathfrak{P}(S_1^{sh})_{\mathfrak{P}} = (X - X')$ and so S_1^{sh} is regular at \mathfrak{P} by Lemma 2.1.

We still have to deal with the second affine open subscheme $U_2^{sh} = \text{Spec } S_2^{sh}$, where $S_2^{sh} = S_2 \otimes_R R^{sh}$. It suffices to check the regularity of S_2^{sh} at the prime ideal

$$(3.12) \quad \mathfrak{P} = (W_2, F_m, \pi),$$

which corresponds to the component F_m in Figure 1. But in S_2^{sh} we even have $\mathfrak{P} = (W_2)$ by Proposition 3.5, and so this ring is obviously regular at \mathfrak{P} . \square

3.3. Resolving the singularities of $\tilde{\mathcal{X}}$. We now find the singular closed points of the normal scheme $\tilde{\mathcal{X}}$ and then resolve these singularities. We shall see that for the resolution it sufficed to blow up the lines that have singular points lying on them. Since blowing up commutes with flat morphisms, we can work with $\tilde{\mathcal{X}}^{sh}$ instead of $\tilde{\mathcal{X}}$ throughout, as long as we only blow up along ideal sheaves \mathcal{I} of $\tilde{\mathcal{X}}^{sh}$ which are of the form $\mathcal{I}\mathcal{O}_{\tilde{\mathcal{X}}^{sh}}$, where \mathcal{I} is an ideal sheaf of $\tilde{\mathcal{X}}$. Before we come to the main result of this section we need to introduce some further terminology. We continue to use the notation of Proposition 3.7.

Definition 3.8. We call a component $L_{(x,y)}$ of $\tilde{\mathcal{X}}^{sh} = \tilde{\mathcal{X}} \times_{\text{Spec } R} \text{Spec } R^{sh}$ a *component of type A*, if $x = 0$ or $x^m = 1$, and a *component of type B*, if x is a multiple root of $\bar{\psi}(X^m, 1 - X^m)$ different from 0.

We first find and resolve the singularities on \mathcal{X}^{sh} . In the following, we call a curve of genus 0 over $\overline{\mathbb{F}}_p$ a *line*.

Theorem 3.9. Let $\tilde{\mathcal{X}}^{sh}$ be the normal scheme given by (3.10). If we blow up $(m-1)$ -times along the components of type A, we get p chains consisting of $(m-1)$ lines (Figure 2). Blowing up along the components of type B gives p chains consisting of one line (Figure 3). The resulting scheme is regular.

For the proof of the theorem we first need three preparatory lemmata.

Lemma 3.10. In the notation of Proposition 3.7, the only singular points of $\tilde{\mathcal{X}}^{sh}$ lie on the components $L_{(x,y)}$ of type A and of type B (Figure 4).

Proof: We first use the Jacobian criterion to locate the singular points on the affine open subset

$$U_1^{sh} \times_{\text{Spec } R^{sh}} \text{Spec } \overline{\mathbb{F}}_p = \text{Spec } (\overline{\mathbb{F}}_p[X, Y, W_1] / (F_m, \psi(X^m, 1 - X^m))) ,$$

see (3.11). The Jacobian matrix is of the form

$$J(X, Y, W_1) = \begin{pmatrix} mX^{m-1} & mY^{m-1} & 0 \\ G'(X) & 0 & 0 \end{pmatrix} ,$$

where $G(X) = \bar{\psi}(X^m, 1 - X^m)$. It follows that a closed point $P = (x, y, w) \in U_1 \times_{\text{Spec } R} \text{Spec } \overline{\mathbb{F}}_p$ is singular if and only if

$$-my^{m-1}G'(x) = 0 .$$

Now $y = 0$ implies $x^m - 1 = 0$, and so x is an m -th root of unity. In case $G'(x) = 0$, the element x is an m -th root of an element of \mathbb{F}_p^* or 0 by Corollary 3.2.

Note that F_m is the only component of the special fiber of $\tilde{\mathcal{X}}^{sh}$ which does not lie in U_1^{sh} . To find its singular points, we work on the affine open subset U_2^{sh} . A closed point which lies on F_m corresponds to a maximal ideal

$$\mathfrak{m} = (\pi, W_2, X - X', Y - Y') \subset S_2^{sh} ,$$

where $X'^m + Y'^m \equiv 1 \pmod{\pi}$, cf. (3.12). Without loss of generality we may again assume $\pi \nmid Y'$. Using arguments similar to those in the proof of Proposition 3.7 combined with (3.9), we see that in S_2^{sh} we have

$$(Y - Y')\epsilon' \in (\pi, W_2, X - X') \subset S_2^{sh} ,$$

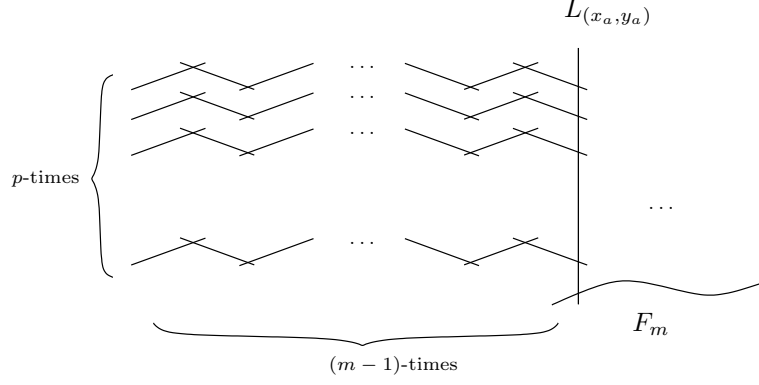


FIGURE 2. The configuration of the components after $(m-1)$ -times blowing up a component $L_{(x_a, y_a)}$ of type A.

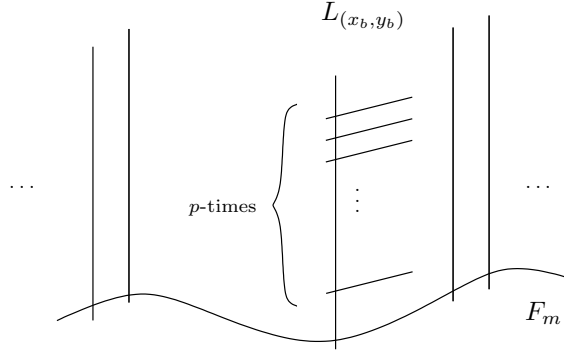


FIGURE 3. The configuration of the components after blowing up a component $L_{(x_b, y_b)}$ of type B.

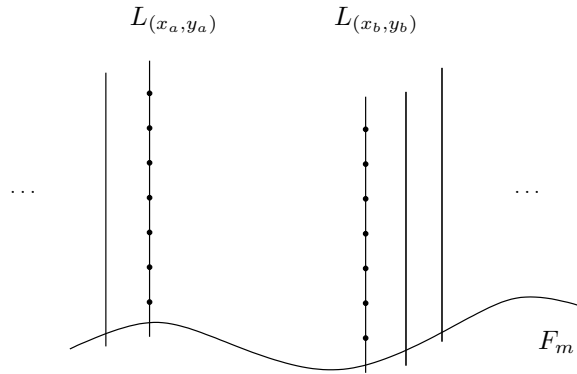
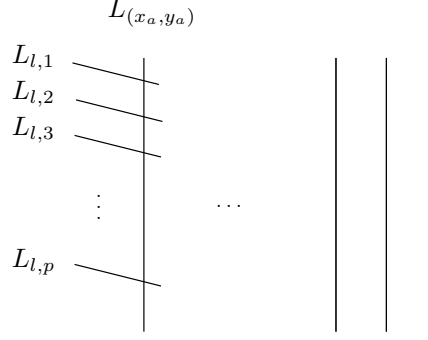


FIGURE 4. The line $L_{(x_a, y_a)}$ is of type A and the line $L_{(x_b, y_b)}$ is of type B.

where $\epsilon' = \prod_{i=1}^{m-1} (Y - Y' \zeta_m^i) \notin \mathfrak{m}$. Together with the fact that $\pi = W_2 F_m$ in S_2^{sh} , this gives us

$$\mathfrak{m}(S_2^{sh})_{\mathfrak{m}} = (W_2, X - X') ;$$


 FIGURE 5. The configuration of the special fiber of $U_{1,l}$.

hence S_2^{sh} is regular at \mathfrak{m} by Lemma 2.1. Therefore there are no singular points lying on components which are not of type A or of type B . \square

Lemma 3.10 shows us that we have to focus on the components of type A and of type B . Let us analyze the former. A component $L_{(x_a, y_a)}$ of type A corresponds to a prime ideal

$$\mathfrak{P} = (\pi, X, Y - \zeta_m^i) \subset S_1^{sh}.$$

There is an affine open neighborhood U of \mathfrak{P} with the property that $V(\mathfrak{P}) \subset U = \text{Spec } A \subseteq U_1^{sh}$ and $\mathfrak{P}A = (\pi, X)$. To be more precise, we have $Y^m - 1 = (Y - \zeta_m^i)f$, where f is the product of the $(Y - \zeta_m^j)$ with $j \neq i$. Then we may take A to be

$$(3.13) \quad A = S/(\pi W_1^p + \mu\psi(X^m, Y^m)),$$

where

$$S = \left(R^{sh}[X, Y, W_1]/(F_m - W_1\pi) \right)_f$$

is the localization of $R^{sh}[X, Y, W_1]/(F_m - W_1\pi)$ with respect to the set $\{1, f, f^2, f^3, \dots\}$. Hence U is isomorphic to the principal open subset $D(f)$ of U_1^{sh} . Note that, as \mathfrak{P} is a regular prime ideal of height one, it is possible to find an affine open neighborhood U' so that \mathfrak{P} is generated by one element in this neighborhood. Unfortunately U' does not contain $V(\mathfrak{P})$.

Next, we study schemes which naturally appear as blow-ups of the scheme $\text{Spec } A$.

Lemma 3.11. *Let $l \in \mathbb{N}$ with $1 \leq l \leq m - 1$ and*

$$(3.14) \quad A_l := S[T_l]/(\pi - T_l X^l, g_l(T_l)),$$

where

$$(3.15) \quad g_l(T_l) = T_l W_1^p + \mu \frac{\psi(X^m, 1 - X^m)}{X^l} + \mu \sum_{k=1}^{p-1} \binom{p}{k} p^{-1} (T_l W_1)^{p-k} X^{l(p-k-1)} Y^{mk} (-1)^k.$$

Furthermore, let $U_{1,l} = \text{Spec } A_l$. Then $U_{1,l}$ is normal; the configuration of the special fiber of $U_{1,l}$ is given in Figure 5. The only components of the special fiber which correspond to prime ideals that contain X are given by $L_{l,1}, \dots, L_{l,p}$ and $L_{(x_a, y_a)}$. If $l = m - 1$, there are no singular closed points lying on these components. If $l < m - 1$, the only singular closed points are the points where the components $L_{l,i}$ intersect the component $L_{(x_a, y_a)}$.

Proof: First of all note that $U_{1,l}$ is a closed subscheme of the regular integral scheme $V_l = \operatorname{Spec} S[T_l]/(\pi - T_l X^l)$. To see that V_l is integral and regular one may observe that even the ring

$$B = R^{sh}[X, Y, W_1, T_l]/(F_m - W_1\pi, \pi - T_l X^l)$$

has these properties: We have that π, X^l is a regular sequence in the integral ring $R^{sh}[X, Y, W_1]/(F_m - W_1\pi)$, so the ring B is one of the rings we get if we blow up $R^{sh}[X, Y, W_1]/(F_m - W_1\pi)$ along the ideal (π, X^l) , see Lemma 2.12. It follows that B is integral by Lemma 2.9. To see the regularity we use the Jacobian criterion and find that the only maximal ideals which can be singular are of the form

$$\mathfrak{m} = (\pi, X, Y - \zeta_m^i, T - T', W_1 - W'),$$

where $T', W' \in R^{sh}$ and $i \in \mathbb{Z}$. We have the chain of prime ideals

$$0 \subsetneq (\pi, X, Y - \zeta_m^i) \subsetneq (\pi, X, Y - \zeta_m^i, T - T') \subsetneq \mathfrak{m}.$$

On the other hand, $\mathfrak{m}B_{\mathfrak{m}} = (X, T - T', W_1 - W')$. This gives us $3 \leq \dim B_{\mathfrak{m}} \leq \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2 \leq 3$, hence the regularity of $B_{\mathfrak{m}}$. It follows from Lemma 2.3 that B is regular.

Let us return to the scheme $U_{1,l}$ and show that it is normal. In order to do this we may first consider the affine open subscheme $U'_{1,l} = \operatorname{Spec}(A_l)_X$, where $(A_l)_X$ is the localization of A_l with respect to the set

$$\{1, X, X^2, X^3, \dots\}.$$

The special fibers of $U'_{1,l}$ and of $U_{1,l}$ have the same configuration, except that $U'_{1,l}$ does not include components corresponding to prime ideals that contain X and π . An easy computation shows that $(A_l)_X \cong (S_1^{sh})_{Xf} = (S_1 \otimes_R R^{sh})_{Xf}$ (cf. (3.8)), where Xf is the multiplicative subset $\{1, f, X, Xf, X^2, f^2, \dots\}$. It follows that $U'_{1,l}$ is normal and that its special fiber has the same configuration as the special fiber of $U_1^{sh} = \operatorname{Spec} S_1^{sh}$ after removing the components $L_{(x,y)}$ with $x = 0$, cf. Proposition 3.7.

Next, let us analyze the components of the special fiber of $U_{1,l}$ that do not lie in $U'_{1,l}$. For a prime ideal $\mathfrak{P} \subset A_l$ such that $\pi, X \in \mathfrak{P}$ we have

$$(3.16) \quad T_l W_1^p + \mu T_l W_1 (\zeta_m^i)^{m(p-1)} = T_l W_1 (W_1^{p-1} + \mu) \in \mathfrak{P},$$

hence the only prime ideals of height one with this property are

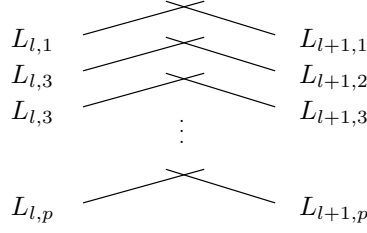
$$(\pi, X, T_l), \quad (\pi, X, W_1), \quad \text{and} \quad (\pi, X, W_1 - \theta \zeta_{p-1}^i),$$

where $0 \leq i \leq p-2$ and θ is an element of R^{sh} satisfying $\theta^{p-1} = -\mu$. Note that \mathfrak{P} can only contain one of the elements T_l , W_1 or $W_1 - \theta \zeta_{p-1}^i$, because otherwise $\mathfrak{P} = A_l$ or \mathfrak{P} is a maximal ideal, hence it is of height 2. Since $\pi = T_l X^l$ in A_l it follows from (3.15) and (3.16) that $\mathfrak{P}(A_l)_{\mathfrak{P}} = (X)$, and therefore that $U_{1,l}$ is normal.

Let $\mathfrak{m} = (X, T_l - T', W_1 - W')$ be a maximal ideal of A_l such that $\pi \nmid T'$ (note that $\pi \in \mathfrak{m}$ since $\pi = T_l X^l$ in A_l). It follows from (3.15) and (3.16) that $T' W_1 (W_1^{p-1} + \mu) \in \mathfrak{m}$ and so we may assume without loss of generality that $W' = 0$ or $W' = \theta \zeta_{p-1}^i$. Since the factors

$$(3.17) \quad W_1, (W_1 - \theta), (W_1 - \theta \zeta_{p-1}), (W_1 - \theta \zeta_{p-1}^2), \dots, (W_1 - \theta \zeta_{p-1}^{p-2})$$

are pairwise coprime, (3.15) and (3.16) show us that $(W_1 - W')$ is contained in the ideal of $(A_l)_{\mathfrak{m}}$ which is generated by X and $(T - T')$. Hence the ring A_l is regular at \mathfrak{m} . Next, let $\mathfrak{m} = (X, T_l, W_1 - W')$, where $(W_1 - W')$ is coprime to all of the factors in (3.17). Then $W_1(W_1^{p-1} + \mu)$ becomes a unit in the localization with respect to \mathfrak{m} . Again, (3.15) and (3.16) yield $\mathfrak{m}(A_l)_{\mathfrak{m}} = (X, W_1 - W')$ and therefore the regularity of A_l at \mathfrak{m} .


 FIGURE 6. The configuration of $\text{Spec } \tilde{A}_{l+1} \times_{\text{Spec } R^{sh}} \text{Spec } \overline{\mathbb{F}}_p$.

Finally, we consider the case $\mathfrak{m} = (X, T_l, W_1 - W')$, where $W' = 0$ or $W' = \theta \zeta_{p-1}^i$ for some integer $0 \leq i \leq p-2$. We may distinguish here between two cases. In case $l = m-1$, we have

$$(3.18) \quad -T_{(m-1)}W_1(W_1^{p-1} + \mu) = \mu X \left(\frac{\psi(X^m, 1 - X^m)}{X^m} + P(T_{(m-1)}) \right)$$

in $A_{(m-1)}$; here $P(T_{(m-1)}) \in S[T_{(m-1)}]$ is the polynomial given by

$$P(T_{(m-1)}) = \sum_{k=1}^{p-2} \frac{\binom{p}{k}}{p} (T_{(m-1)}W_1)^{p-k} X^{(m-1)(p-k-1)-1} Y^{mk} (-1)^k.$$

Obviously we have $P(T_{(m-1)}) \in \mathfrak{m}$. If the term in parentheses on the right-hand side of (3.18) were contained in \mathfrak{m} , then we would have

$$\frac{\psi(X^m, 1 - X^m)}{X^m} \in \mathfrak{m},$$

a contradiction. Hence this term becomes a unit in $(A_{(m-1)})_{\mathfrak{m}}$, and we have

$$\mathfrak{m}(A_{(m-1)})_{\mathfrak{m}} = (T_{(m-1)}, W_1 - W').$$

In other words, $A_{(m-1)}$ is regular at \mathfrak{m} .

Now consider the case $l < m-1$. Let \mathfrak{M} be the prime ideal of the regular ring $S[T_l]/(\pi - T_l X^l)$ which is given by the preimage of \mathfrak{m} . Since $(Y - \zeta_m^i) = -(X^m - W_1 T_l X^l) f^{-1}$ in $S[T_l]/(\pi - T_l X^l)$, we have $(Y - \zeta_m^i) \in \mathfrak{M}^2$, which yields

$$g_l(T_l) \equiv T_l W_1^p + \mu T_l W_1 \equiv 0 \pmod{\mathfrak{M}^2}.$$

Hence A_l is singular at \mathfrak{m} . Let us denote the components which correspond to the prime ideals (π, X, W_1) and $(\pi, X, W_1 - \theta \zeta_{p-1}^i)$ for $0 \leq i \leq p-2$ by $L_{l,1}, \dots, L_{l,p}$. The configuration of $U_{1,l} \times_{\text{Spec } R^{sh}} \text{Spec } \overline{\mathbb{F}}_p$ is given in Figure 5. \square

Lemma 3.12. *We use the notation from Lemma 3.11. Let $l < m-1$. If we blow up along the ideal (X, T_l) the resulting scheme is covered by the affine open subset $U_{1,l+1}$ (cf. Lemma 3.11) and an affine open subset $\tilde{U}_{l+1} = \text{Spec } \tilde{A}_{l+1}$. The configuration of the special fiber is given by Figure 5 (replacing l by $l+1$) in $U_{1,l+1}$ and by Figure 6 in \tilde{U}_{l+1} . The scheme \tilde{U}_{l+1} is regular.*

Proof: We blow up along the ideal (X, T_l) . Setting $\frac{X}{T_l} = \tilde{X}$, one affine open subset of the blow-up is isomorphic to $\text{Spec } \tilde{A}_{l+1}$, where

$$\tilde{A}_{l+1} := S[T_l, \tilde{X}] / (\pi - T_l^{l+1} \tilde{X}^l, \tilde{X} T_l - X, \tilde{g}_l(\tilde{X})) \cong A_l [X T_l^{-1}] ,$$

and

$$\begin{aligned} \tilde{g}_l(\tilde{X}) &= W_1^p + \mu \frac{\psi((\tilde{X} T_l)^m, 1 - (\tilde{X} T_l)^m)}{\tilde{X}^l T_l^{l+1}} \\ &\quad + \mu \sum_{k=1}^{p-1} \binom{p}{k} p^{-1} T_l^{(l+1)(p-k-1)} \tilde{X}^{l(p-k-1)} W_1^{p-k} Y^{mk} (-1)^k . \end{aligned}$$

A prime ideal I which contains π also contains X and $Y - \zeta_m^i$, since $T_l \in I$ or $\tilde{X} \in I$. Furthermore, in case $\tilde{X} \in I$, we have $W_1^p + \mu W_1 \in I$. Hence, the prime ideals of height 1 which contain \tilde{X} are of the form $(\tilde{X}, G(W_1))$, where $G(W_1)$ is one of the factors in (3.17). We denote these prime ideals by $\mathfrak{P}_1, \dots, \mathfrak{P}_p$. In case $T_l \in I$ we have $W_1^p + \mu W_1 \in I$ as well. We denote the prime ideals $(T_l, G(W_1))$ by $\mathfrak{Q}_1, \dots, \mathfrak{Q}_p$. A maximal ideal \mathfrak{m} of \tilde{A}_{l+1} is of the form $\mathfrak{m} = (\tilde{X}, G(W_1), T_l - T')$ ($\mathfrak{m} = (T_l, G(W_1), \tilde{X} - X')$ resp.). If we localize with respect to this ideal, the corresponding ideal in the localization is generated by \tilde{X} and $T_l - T'$ (T_l and $\tilde{X} - X'$ resp.), hence the ring is regular at \mathfrak{m} . Since these are the only maximal ideals of this ring, the ring itself is regular by Lemma 2.3. The blow-up-morphism $\tilde{U}_{l+1} = \text{Spec } \tilde{A}_{l+1} \rightarrow \text{Spec } A_l$ is an isomorphism away from $V(X, T_l)$. The components $L_{l,i}$ of $U_{1,l}$ are the images of the components which correspond to the prime ideals $\mathfrak{P}_i \subset \tilde{A}_{l+1}$. Therefore we denote these components by $L_{l,i}$ as well. The components which lie above the singular points are denoted by $L_{l+1,i}$. They correspond to the prime ideals \mathfrak{Q}_i . Then the special fiber has the configuration as in Figure 6. The component $L_{l,i}$ intersects the component $L_{l+1,i}$ in the point corresponding to some $\mathfrak{m} = (\tilde{X}, T_l, G(W_1))$.

Let us now take a look at the other affine open subset of the blow-up. Setting $T_{l+1} = \frac{T_l}{X}$, we get

$$A_l [T_l X^{-1}] \cong S[T_l, T_{l+1}] / (\pi - T_{l+1} X^{l+1}, T_{l+1} X - T_l, g_{l+1}(T_{l+1})) = A_{l+1} .$$

Note that the components $L_{l+1,i}$ of $U_{1,l+1} = \text{Spec } A_{l+1}$ are the components $L_{l+1,i}$ of $\text{Spec } \tilde{A}_{l+1}$. \square

Proof of Theorem 3.9: According to Lemma 3.10 the only singular points are closed points on the components of type A and type B . Let $L_{(x_a, y_a)}$ be a component of type A that corresponds to a prime ideal $\mathfrak{P} = (\pi, X, Y - \zeta_m^i) \subset S_1^{sh}$. We work in the affine open subset $U = \text{Spec } A$, where A is the ring of (3.13). We blow up U along $V(\mathfrak{P}A)$. Since $\mathfrak{P}A = (\pi, X)$, the blow-up is covered by two affine open subsets. Setting $T_1 = \frac{\pi}{X}$, the first one is given by $U_{1,1}$. The only new components are $L_{1,1}, \dots, L_{1,p}$, cf. Figure 5 with $l = 1$. Setting $X_1 = \frac{X}{\pi}$, the second subset is

$$\text{Spec } S[X_1] / (X_1 \pi - X, g(X_1)) ,$$

where

$$g(X_1) = W_1^p + \mu \frac{\psi((X_1 \pi)^m, 1 - (X_1 \pi)^m)}{\pi} + \mu \sum_{k=1}^{p-1} \binom{p}{k} p^{-1} W_1^{p-k} \pi^{p-k-1} Y^{mk} (-1)^k .$$

Here we only have to study the prime ideals \mathfrak{m} such that $X_1, \pi \in \mathfrak{m}$, since all the others that lie above π can be found in $U_{1,1}$. We have

$$W_1^p + \mu W_1 = \pi P(X_1)$$

in $S[X_1]/(X_1\pi - X, g(X_1))$, where $P(X_1) \in S[X_1]$. It follows that $W_1^p + \mu W_1 \in \mathfrak{m}$, which implies

$$(3.19) \quad W_1 \in \mathfrak{m} \text{ or } W_1 - \theta \zeta_{p-1}^i \in \mathfrak{m}$$

for some $0 \leq i \leq p-2$; here $\theta \in R^{sh}$ satisfies $\theta^{p-1} = -\mu$. The prime ideal \mathfrak{m} is of the form $\mathfrak{m} = (\pi, X_1, W_1)$ ($\mathfrak{m} = (\pi, X_1, W_1 - \theta \zeta_{p-1}^i$ resp.), hence maximal. In fact, they are the “end points” of the components $L_{1,i}$. Since the factors in (3.19) are pairwise coprime,

$$\mathfrak{m}(S[X_1]/(X_1\pi - X, g(X_1)))_{\mathfrak{m}}$$

is generated by two elements, hence $S[X_1]/(X_1\pi - X, g(X_1))$ is regular at \mathfrak{m} . There are p singular closed points lying on $L_{(x_a, y_a)}$ (Lemma 3.11). If we blow up this line, we get further components $L_{2,1}, \dots, L_{2,p}$ by Lemma 3.12. There are no singular closed points lying on the $L_{1,i}$, see Lemma 3.12. Lemma 3.11 implies that the only singular closed points that lie on the $L_{2,i}$ or the line $L_{(x_a, y_a)}$ are the points where the $L_{2,i}$ intersect $L_{(x_a, y_a)}$. It is clear that repeating this process (i.e. blowing up the component $L_{(x_a, y_a)}$) $m-3$ times gives the resolution of the singularities that lie on this component, and therefore yields the configuration we claimed. By symmetry we can argue analogously for components of type A which correspond to prime ideals of the form $\mathfrak{P} = (\pi, X - \zeta_m^i, Y)$.

Finally, a similar (but simpler, since no inductive argument is needed) computation shows that we have to blow up the components of type B only once, yielding the remaining assertions of the lemma. \square

3.4. The configuration of the geometric special fiber of the local minimal regular model. Having located and resolved the singularities of \mathcal{X}^{sh} , we can now describe the minimal regular model of F_N over R .

Theorem 3.13. *Let N be an odd squarefree natural number which has at least two prime factors, ζ_N a primitive N -th root of unity and $N = pm$, where p is prime and $m \in \mathbb{N}$. Furthermore, let R be the localization of $\mathbb{Z}[\zeta_N]$ with respect to a fixed prime ideal $\mathfrak{p} \in \text{Spec } \mathbb{Z}[\zeta_N]$ that lies above p . We denote by $\mathfrak{F}_{N,\mathfrak{p}}^{min} \rightarrow \text{Spec } R$ the minimal regular model of the Fermat curve F_N over R . Then the geometric special fiber*

$$\mathfrak{F}_\pi := \mathfrak{F}_{N,\mathfrak{p}}^{min} \times_{\text{Spec } R} \text{Spec } \overline{\mathbb{F}}_p$$

has the configuration as in Figure 7; Table 1 contains the number, multiplicity, genus and self-intersection of the components. Finally, all intersection between components of the geometric special fiber are transversal.

Proof: The scheme

$$\mathfrak{F}_{N,\mathfrak{p}}^0 = \text{Proj } R[X_0, Y_0, Z_0]/(X_0^N + Y_0^N - Z_0^N)$$

is covered by the affine scheme \mathcal{X} in (3.1) and by

$$\mathcal{X}' = \text{Spec } R[Y', Z']/(1 + Y'^N - Z'^N),$$

where $Y' = \frac{Y_0}{X_0}$ and $Z' = \frac{Z_0}{X_0}$. To blow up $\mathfrak{F}_{N,\mathfrak{p}}^0$ along the ideal $V_+(X_0^m + Y_0^m - Z_0^m, \pi)$ is to blow up \mathcal{X} along (π, F_m) and \mathcal{X}' along $(\pi, 1 + Y'^m - Z'^m)$ and then glue the resulting

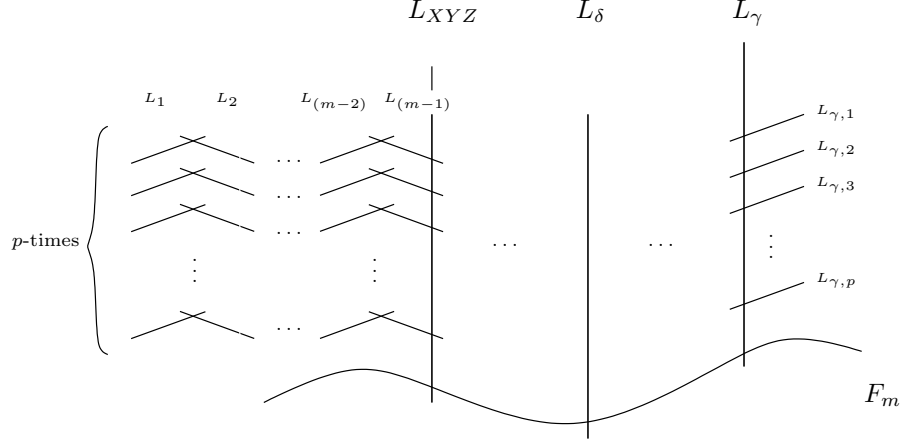


FIGURE 7. The configuration of the geometric special fiber \mathfrak{F}_π .

	Number of components	Multiplicity	Genus	Self-intersection
L_i	$3mp$	i	0	-2
L_{XYZ}	$3m$	m	0	$-p$
L_γ	$m\rho$	2	0	$-p$
$L_{\gamma,j}$	$pm\rho$	1	0	-2
L_δ	$m^2(p-3) - 2m\rho$	1	0	$-p$
F_m	1	p	$\frac{1}{2}(m-1)(m-2)$	$-m^2$

TABLE 1. ρ denotes the number of factors with multiplicity two of $\Psi(X^m)$ over \mathbb{F}_p (cf. Definition 3.3).

schemes together; we denote these blow-ups by $\tilde{\mathcal{X}}$ and $\tilde{\mathcal{X}}'$. As \mathcal{X} is isomorphic to \mathcal{X}' and (π, F_m) to $(\pi, 1 + Y'^m - Z'^m)$ via $X \mapsto Z'$ and $Y \mapsto -Y'$, the blow-ups $\tilde{\mathcal{X}}$ and $\tilde{\mathcal{X}}'$ are isomorphic as well. The only components of $\tilde{\mathcal{X}}'$ which are not in $\tilde{\mathcal{X}}$ are the ones corresponding to prime ideals that contain Z' . Under the isomorphism above these components correspond to the components of type A which contain X . It follows that we can apply Theorem 3.9 to resolve the singularities of these schemes. The regular model of F_N we obtain in this way will be denoted by $\mathfrak{F}_{N,p}$. By the discussion above, it is enough to analyze the regular scheme from Theorem 3.9, remembering that there are a few more components which we cannot see in this affine open subset. We sketch how the quantities in Table 1 can be derived. In fact, we compute these quantities for the model $\mathfrak{F}_{N,p}$, we will see later that in fact $\mathfrak{F}_{N,p} = \mathfrak{F}_{N,p}^{\min}$.

Let us start with the number of components of $\mathfrak{F}_{N,p}$. By Theorem 3.9 it is clear that the geometric special fiber of $\mathfrak{F}_{N,p}$ has the configuration depicted in Figure 7. The vertical components are parametrized by pairs $(x, y) \in \mathbb{F}_p$ with $x^m + y^m - 1 = x^m \prod_{i=0}^{m-1} (x - \bar{\zeta}_m^i) \bar{\Psi}(x^m) = 0$, see Proposition 3.7. There are ρ factors $(X - \bar{\gamma}_k)^2$ in $\bar{\Psi}(X^m)$, and for each $\bar{\gamma}_k$ the polynomial $Y^m + \bar{\gamma}_k^m - 1 \in \mathbb{F}_p[Y]$ has m solutions, as $\bar{\gamma}_k^m \neq 1$. Hence we get $m\rho$ lines. We denote these lines by L_γ ; they are the ones of type B in Theorem 3.9. Furthermore, there are $m(p-3) - 2\rho$ linear factors $(X - \bar{\delta})$ and with the same argument as before there are $m(m(p-3) - 2\rho)$ lines which correspond to these. We denote these by L_δ .

The only solutions which are left are the following:

$$(3.20) \quad (0, \bar{\zeta}_m^i)$$

for $0 \leq i \leq m-1$, and

$$(3.21) \quad (\bar{\zeta}_m^i, 0)$$

for $0 \leq i \leq m-1$. This gives us $2m$ lines; they are the components of type A in Theorem 3.9. However, as mentioned above, there are more lines which behave like the ones of type A but which cannot be seen in this affine picture. In fact, by the isomorphism we described at the beginning of the proof, it is clear that there are m more lines, hence these, together with the ones of (3.20) and (3.21), give us $3m$ lines. We denote them by L_{XYZ} . According to Theorem 3.9, for each L_{XYZ} there are p chains of $m-1$ lines, where the ends of the chains intersect L_{XYZ} . These ends are denoted by $L_{(m-1)}$ and the following lines by $L_{(m-2)}, L_{(m-3)}$, etc. Also by Theorem 3.9, there are p lines intersecting each L_γ . We denote these lines by $L_{\gamma,1}, \dots, L_{\gamma,p}$. Collecting this information we get the number of components of table 1.

Next, we want to study the multiplicity of the components in the geometric special fiber \mathfrak{F}_π , see [Liu, Definition 7.5.6]. We illustrate this only in a few cases. For example, let us return to the scheme $U_{1,l} = \text{Spec } A_l$ in (3.14). The prime ideals of height 1 of A_l are (π, X, W_1) and $(\pi, X, W_1 - \theta \zeta_{p-1}^i)$ for $0 \leq i \leq p-2$. These correspond to the components L_l . Furthermore, there is the prime ideal (π, X, T_l) which corresponds to a component L_{XYZ} , after blowing up $m-1-l$ times. Let \mathfrak{P} be a prime ideal that corresponds to L_l . In Theorem 3.9 we have seen that $\mathfrak{P}(A_l)_{\mathfrak{P}} = (X)$. Since $\pi = T_l X^l$ in A_l and T_l becomes a unit in $(A_l)_{\mathfrak{P}}$, we get $\nu_{L_l}(\pi) = l$, hence the multiplicity of L_l is l . Now let $\mathfrak{P} = (\pi, X, T_l)$. Equation (3.15) shows $T_l = X^{m-l} \epsilon$ in $(A_l)_{\mathfrak{P}}$, where $\epsilon \in (A_l)_{\mathfrak{P}}^*$. With the same argument as before we get $\nu_{L_{XYZ}}(\pi) = m$, hence the component L_{XYZ} has multiplicity m . The multiplicities of the other components can be computed in a similar way. The genera of the components are obvious.

We now prove that all intersections are transversal. Let \mathcal{T} denote the set of irreducible components of \mathfrak{F}_π . Then we have

$$\mathfrak{F}_\pi = \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}} \mathcal{C},$$

where $d_{\mathcal{C}}$ is the multiplicity of \mathcal{C} in \mathfrak{F}_π . For a component $\mathcal{C} \in \mathcal{T}$, we have

$$0 < \mathcal{C}(\mathfrak{F}_\pi - d_{\mathcal{C}} \mathcal{C}).$$

Let us denote by $I_{\mathcal{C}}$ the sum of the multiplicities of the components that have a positive intersection number with \mathcal{C} . Obviously we have

$$I_{\mathcal{C}} \leq \mathcal{C}(\mathfrak{F}_\pi - d_{\mathcal{C}} \mathcal{C}),$$

and equality holds for all \mathcal{C} if and only if all intersections are transversal. We get the following table:

\mathcal{C}	$I_{\mathcal{C}}$
L_i	$2i$
L_{XYZ}	$p + p(m-1)$
L_γ	$2p$
$L_{\gamma,j}$	2
L_δ	p
F_m	$m^2 p$

Let us denote by \mathcal{K} a canonical divisor of $\mathfrak{F}_{N,p}$. By the adjunction formula (cf. Theorem 2.17) and by properties of the intersection matrix of \mathfrak{F}_π (see for instance [Liu, Proposition 8.1.21, Proposition 8.1.35]) we have

$$\begin{aligned}
2g_a(F_N) - 2 &= \mathcal{K} \cdot \mathfrak{F}_\pi \\
&= \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}}(\mathcal{K} \cdot \mathcal{C}) \\
&= \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}}(-\mathcal{C}^2 + 2g_a(\mathcal{C}) - 2) \\
&= \sum_{\mathcal{C} \in \mathcal{T}} \mathcal{C}(\mathfrak{F}_\pi - d_{\mathcal{C}}\mathcal{C}) + 2pg_a(F_m) - 2 \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}} \\
&\geq \sum_{\mathcal{C} \in \mathcal{T}} I_{\mathcal{C}} + 2pg_a(F_m) - 2 \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}};
\end{aligned}$$

hence the intersections are transversal if and only if

$$(3.22) \quad 2g_a(F_N) - 2 = \sum_{\mathcal{C} \in \mathcal{T}} I_{\mathcal{C}} + 2pg_a(F_m) - 2 \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}}.$$

Using the quantities of Table 1 and the table for the $I_{\mathcal{C}}$ we get

$$\sum_{\mathcal{C} \in \mathcal{T}} I_{\mathcal{C}} = 3m^3p - 2m^2p + 2pm\rho + m^2p^2$$

and

$$-2 \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}} = -3m^3p + m^2p - 2pm\rho - 2p.$$

We have

$$2g_a(F_N) - 2 = m^2p^2 - 3mp$$

and

$$\begin{aligned}
\sum_{\mathcal{C} \in \mathcal{T}} I_{\mathcal{C}} - 2 \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}} + 2pg_a(F_m) &= -m^2p + m^2p^2 - 2p + p(m-1)(m-2) \\
&= m^2p^2 - 3mp,
\end{aligned}$$

which yields (3.22) and therefore the transversality of the intersections.

Since we know the intersection numbers and the configuration of the geometric special fiber, one can use that $(\mathcal{C} \cdot \mathfrak{F}_\pi) = 0$ to get the self-intersection number of a component $\mathcal{C} \in \mathcal{T}$.

Finally, since there are no exceptional divisors by Castelnuovo's criterion [Liu, Theorem 9.3.8], $\mathfrak{F}_{N,p}$ is already the minimal regular model. \square

Remark 3.14. If we consider the case $m = 1$, so that $N = p$ is prime, then the model constructed in Theorem 3.13 remains regular. However, the component $F_m = F_1$ is an exceptional divisor, so the model is not minimal. Contracting F_1 yields the minimal regular model of F_p over R , see [Mc].

We can use Theorem 3.13 to analyze the singularities of the normalization $\mathfrak{F}_{N,p}^{nor}$ of the scheme

$$\mathfrak{F}_{N,p}^0 = \text{Proj } R[X, Y, Z]/(X^N + Y^N - Z^N).$$

Recall that a normal and excellent two-dimensional scheme \mathcal{X} has *rational singularities*, if for one (and hence every) desingularization $f : \mathcal{X}' \rightarrow \mathcal{X}$, we have

$$R^i f_* \mathcal{O}_{\mathcal{X}'} = 0$$

for all $i > 0$. See [Art].

Corollary 3.15. *The normal scheme $\mathfrak{F}_{N,\mathfrak{p}}^{\text{nor}}$ has rational singularities.*

Proof: It follows from the proofs of Theorems 3.9 and 3.13 that there is a desingularization $f^{\text{nor}} : \mathfrak{F}_{N,\mathfrak{p}}^{\text{min}} \rightarrow \mathfrak{F}_{N,\mathfrak{p}}^{\text{nor}}$. Let $P \in \mathfrak{F}_{N,\mathfrak{p}}^{\text{nor}}$ be a singular point and $\mathcal{C}_1, \dots, \mathcal{C}_n$ the components of $\mathfrak{F}_{N,\mathfrak{p}}^{\text{min}}$ with $f^{\text{nor}}(\mathcal{C}_i) = P$. According to [Art, Theorem 3], P is a rational singularity if and only if the fundamental cycle \mathcal{Z}_P with respect to P , also defined in [Art], satisfies $p_a(\mathcal{Z}_P) = 0$. Using Theorem 3.13, we find that

$$\mathcal{Z}_P = \sum_{i=1}^n \mathcal{C}_i.$$

The adjunction formula together with an inductive argument yields

$$p_a(\mathcal{Z}_P) = \sum_{i=1}^n p_a(\mathcal{C}_i) + \sum_{1 \leq i < j \leq n} (\mathcal{C}_i \cdot \mathcal{C}_j) - (n-1) = \sum_{1 \leq i < j \leq n} (\mathcal{C}_i \cdot \mathcal{C}_j) - (n-1).$$

Finally, it is not hard to see – using the configuration described in Theorem 3.13 – that $p_a(\mathcal{Z}_P) = 0$. \square

Remark 3.16. The computation of local minimal regular models of Fermat curves of squarefree even or squareful exponent is more involved. See [Cu, Chapter 7] for a summary of the problems one encounters and possible strategies for dealing with them.

4. THE GLOBAL MINIMAL REGULAR MODEL

Let N be an odd squarefree composite integer. In this section we turn to the global situation; we construct the minimal regular model of F_N over $\mathbb{Z}[\zeta_N]$, where ζ_N is a primitive N -th root of unity. The following result shows that it essentially suffices to localize at the primes \mathfrak{p} of $\mathbb{Z}[\zeta_N]$ dividing N .

Proposition 4.1. *Let \mathcal{X} be the Fermat scheme*

$$\mathcal{X} = \text{Spec } \mathbb{Z}[\zeta_N][X, Y]/(X^N + Y^N - 1).$$

If \mathfrak{p} is a prime ideal of $\mathbb{Z}[\zeta_N]$ not dividing N , then \mathcal{X} is regular at \mathfrak{p} .

Proof: We have a morphism $g : \mathcal{X} \rightarrow \mathcal{Y} = \text{Spec } \mathbb{Z}[\zeta_N]$ which corresponds to the ring homomorphism

$$g^\# : \mathbb{Z}[\zeta_N] \rightarrow \mathbb{Z}[\zeta_N][X, Y]/(X^N + Y^N - 1)$$

where $g^\#$ is the composition of the inclusion $\mathbb{Z}[\zeta_N] \rightarrow \mathbb{Z}[\zeta_N][X, Y]$ and the canonical surjection $\mathbb{Z}[\zeta_N][X, Y] \rightarrow \mathbb{Z}[\zeta_N][X, Y]/(X^N + Y^N - 1)$. The scheme \mathcal{X} is integral, \mathcal{Y} is a Dedekind scheme, and g is non-constant, hence the morphism g is flat, see e.g. [Liu, p.137: Corollary 3.10.]. We want to show that \mathcal{X} is regular at a prime ideal $\mathfrak{p} \in \mathcal{X}$ if $N \notin \mathfrak{p}$. To see this we start with a prime ideal \mathfrak{p} with $g(\mathfrak{p}) = 0$. Then this prime ideal is the image of an element of $\mathcal{X}_{\mathbb{Q}(\zeta_N)} = \text{Spec } \mathbb{Q}(\zeta_N)[X, Y]/(X^N + Y^N - 1)$ with respect to the obvious morphism $\mathcal{X}_{\mathbb{Q}(\zeta_N)} \rightarrow \mathcal{X}$. Since this morphism is flat and $\mathcal{X}_{\mathbb{Q}(\zeta_N)}$ is regular it follows that \mathcal{X} is regular at \mathfrak{p} (see e.g. [Gro, p.143: Corollaire 6.5.2.]. Next, let \mathfrak{p} be a prime ideal with $g(\mathfrak{p}) = \mathfrak{q}$, where \mathfrak{q} is a prime in $\mathbb{Z}[\zeta_N]$. Since \mathcal{Y} is regular, we only have to concentrate on the fiber $\mathcal{X}_{\mathfrak{q}} = \text{Spec } k(\mathfrak{q})[X, Y]/(X^N + Y^N - 1)$,

where $k(\mathfrak{q})$ is the residue field of \mathfrak{q} (Lemma 2.5). We use the Jacobian criterion to analyze the scheme $\mathcal{X}_{\mathfrak{q}}$. For simplicity we may change to the *geometric special fiber* $\overline{\mathcal{X}}_{\mathfrak{q}} = \mathcal{X}_{\mathfrak{q}} \times_{\mathrm{Spec} k(\mathfrak{q})} \mathrm{Spec} \overline{k(\mathfrak{q})} = \mathrm{Spec} \overline{k(\mathfrak{q})}[X, Y]/(X^N + Y^N - 1)$. Since the inclusion morphism $k(\mathfrak{q}) \hookrightarrow \overline{k(\mathfrak{q})}$ is faithfully flat, the projection morphism $p_2 : \overline{\mathcal{X}}_{\mathfrak{q}} \rightarrow \mathcal{X}_{\mathfrak{q}}$ is faithfully flat as well. Hence, if $\overline{\mathcal{X}}_{\mathfrak{q}}$ is regular, then $\mathcal{X}_{\mathfrak{q}}$ is regular, see Remark 2.6. Now let us assume that $N \notin \mathfrak{q}$. Then the rank of the Jacobian matrix $J = (NX^{N-1}, NY^{N-1})$ is 1 for all points of $\overline{\mathcal{X}}_{\mathfrak{q}}$ and so $\overline{\mathcal{X}}_{\mathfrak{q}}$ is regular by the Jacobian criterion and by [Liu, Corollary 4.2.17.], hence \mathcal{X} is regular in \mathfrak{p} (Lemma 2.5). If $N \in \mathfrak{q}$ then the Jacobian matrix is zero and it follows that $\overline{\mathcal{X}}_{\mathfrak{q}}$ is singular at all points. In this situation Lemma 2.5 does not tell us, if \mathcal{X} is regular at \mathfrak{p} . \square

We now use Theorem 3.13 and Proposition 4.1 to determine the minimal regular model of F_N over $\mathbb{Z}[\zeta_N]$. Let $U = \mathrm{Spec} \mathbb{Z}[\zeta_N, 1/N] \subset \mathrm{Spec} \mathbb{Z}[\zeta_N]$ be the open subset consisting of the prime ideals \mathfrak{p} with $N \notin \mathfrak{p}$. We set $\mathfrak{F}_{N,U}^{\min} = \mathfrak{F}_N^0 \times_{\mathrm{Spec} \mathbb{Z}[\zeta_N]} U$, where

$$\mathfrak{F}_N^0 = \mathrm{Proj} \mathbb{Z}[\zeta_N][X, Y, Z]/(X^N + Y^N - Z^N);$$

the scheme $\mathfrak{F}_{N,U}^{\min}$ is regular by Proposition 4.1. For a prime ideal \mathfrak{p} with $N \in \mathfrak{p}$, recall the minimal regular model $\mathfrak{F}_{N,\mathfrak{p}}^{\min}$ from Theorem 3.13, where $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Corollary 4.2. *The minimal regular model \mathfrak{F}_N^{\min} of the Fermat curve F_N over $\mathrm{Spec} \mathbb{Z}[\zeta_N]$ can be obtained by gluing the scheme $\mathfrak{F}_{N,U}^{\min}$ and all the $\mathfrak{F}_{N,\mathfrak{p}}^{\min}$, where \mathfrak{p} runs through all primes of $\mathbb{Z}[\zeta_N]$ dividing N .*

Proof. It follows from general descent theory (cf. [BLR, Chapter 6]) that we can glue $\mathfrak{F}_{N,U}^{\min}$ and the $\mathfrak{F}_{N,\mathfrak{p}}^{\min}$ to get a regular model of F_N over $\mathrm{Spec}(\mathbb{Z}[\zeta_N])$. See [Cu, Corollary 2.3.5] for a precise statement. This model is indeed the minimal regular model, since it contains no exceptional divisors by Castelnuovo's criterion [Liu, Theorem 9.3.8]. \square

PART II: THE ARITHMETIC SELF-INTERSECTION OF THE RELATIVE DUALIZING SHEAF ON THE MINIMAL MODEL OF A FERMAT CURVE OF ODD SQUAREFREE EXPONENT

5. BOUNDING THE ARITHMETIC SELF-INTERSECTION OF THE RELATIVE DUALIZING SHEAF ON ARITHMETIC SURFACES

5.1. Arakelov intersection theory on arithmetic surfaces. Throughout this section we let K be a number field, \mathcal{O}_K its ring of integers and $\pi : \mathcal{X} \rightarrow \operatorname{Spec} \mathcal{O}_K$ an arithmetic surface whose generic fiber X has genus ≥ 2 . See Soulé [So] and [CK] for the definitions and results on intersection multiplicities between hermitian line bundles that we need in the following. In fact, we will only encounter intersection multiplicities between certain special hermitian line bundles. On the one hand, we consider hermitian line bundles $\overline{\mathcal{O}}(V)$, where $V = \sum_{\mathfrak{p}} V_{\mathfrak{p}}$ is a vertical divisor on \mathcal{X} with the sum running over all closed points $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$, and the metric is trivial. For instance, we then have

$$(5.1) \quad \overline{\mathcal{O}}(V)^2 = \sum_{\mathfrak{p}} V_{\mathfrak{p}}^2 \log \operatorname{Nm}(\mathfrak{p}).$$

On the other hand, we consider the hermitian line bundle $\overline{\omega}_{\mathcal{X}} = (\omega_{\mathcal{X}}, \|\cdot\|)$, where $\omega_{\mathcal{X}} = \omega_{\mathcal{X}/\mathcal{O}_K}$ is the relative dualizing sheaf of \mathcal{X} over \mathcal{O}_K and $\|\cdot\|$ is the *Arakelov metric*, i.e. the unique metric on $\omega_{\mathcal{X}}$ such that the Arakelov adjunction formula holds, see [Ara, §4]. The goal of Part II is to bound $\overline{\omega}_{\mathcal{X}}^2$ in terms of N when \mathcal{X} is the minimal regular model of a Fermat curve of odd squarefree exponent N over $\mathbb{Z}[\zeta_N]$.

Remark 5.1. Instead of $\omega_{\mathcal{X}} = \omega_{\mathcal{X}/\mathcal{O}_K}$, some authors prefer to work with the relative dualizing sheaf $\omega_{\mathcal{X}/\mathbb{Z}}$, also equipped with the Arakelov metric. We have

$$\omega_{\mathcal{X}/\mathbb{Z}} = \omega_{\mathcal{X}/\mathcal{O}_K} \otimes \pi^* \omega_{\mathcal{O}_K/\mathbb{Z}},$$

Therefore

$$(5.2) \quad \overline{\omega}_{\mathcal{X}/\mathbb{Z}}^2 = \overline{\omega}_{\mathcal{X}/\mathcal{O}_K}^2 + (2g - 2) \log |\Delta_{K/\mathbb{Q}}|^2,$$

so that bounds on $\overline{\omega}_{\mathcal{X}/\mathcal{O}_K}^2$ are easily translated into bounds on $\overline{\omega}_{\mathcal{X}/\mathbb{Z}}^2$ and vice versa.

5.2. Kühn's upper bound. We first recall a method for the computation of an upper bound on $\omega_{\mathcal{X}}$ due to Kühn [Kü2]. Let $\mathcal{Y} \rightarrow \operatorname{Spec} \mathcal{O}_K$ be an arithmetic surface with generic fiber Y . Fix $\infty, P_1, \dots, P_r \in Y(K)$ such that $Y \setminus \{\infty, P_1, \dots, P_r\}$ is hyperbolic. In this section we assume that the arithmetic surface $\mathcal{X} \rightarrow \operatorname{Spec} \mathcal{O}_K$ comes equipped with a dominant morphism $\beta : \mathcal{X} \rightarrow \mathcal{Y}$ of degree d such that the induced morphism $\beta : X \rightarrow Y$ is unramified outside ∞, P_1, \dots, P_r . We write $\beta^* \infty = \sum b_j S_j$ and set $b_{\max} = \max_j \{b_j\}$. We call a prime \mathfrak{p} *bad* if the fiber $\mathcal{X}_{\mathfrak{p}}$ of \mathcal{X} above \mathfrak{p} is reducible, in which case $\mathcal{X}_{\mathfrak{p}}$ is called a *bad fiber*. Kühn has shown how to bound $\omega_{\mathcal{X}}^2$ in terms of data which depends only on K , on Y , on b_{\max} and on the configuration of the bad fibers of \mathcal{X} .

Let \mathcal{K} be a canonical \mathbb{Q} -divisor of \mathcal{X} . For each S_j we can find a \mathbb{Q} -divisor \mathcal{F}_j such that

$$(5.3) \quad \left(S_j + \mathcal{F}_j - \frac{1}{2g-2} \mathcal{K} \right) \cdot \mathcal{C} = 0$$

for all vertical irreducible components \mathcal{C} of \mathcal{X} . Similarly we can find, for each S_j , a \mathbb{Q} -divisor \mathcal{G}_j such that for all vertical irreducible components \mathcal{C} we have

$$(5.4) \quad \left(S_j + \mathcal{G}_j - \frac{1}{d} \operatorname{div}(s) \right) \cdot \mathcal{C} = 0,$$

where $\overline{\infty}$ is the Zariski closure of ∞ in \mathcal{Y} and s is a section of $\beta^*\mathcal{O}(\infty)$. We define

$$(5.5) \quad \sum_{\mathfrak{p} \text{ bad}} a_{\mathfrak{p}} \log \text{Nm}(\mathfrak{p}) = -\frac{2g}{d} \sum_j b_j \overline{\mathcal{O}}(\mathcal{G}_j)^2 + \frac{2g-2}{d} \sum_j b_j \overline{\mathcal{O}}(\mathcal{F}_j)^2,$$

where the line bundles carry the trivial metric.

Theorem 5.2. *Let $\beta : \mathcal{X} \rightarrow \mathcal{Y}$ be as above. If all S_j are K -rational points and all divisors of degree zero supported in the S_j are torsion, then the arithmetic self-intersection number of the dualizing sheaf $\overline{\omega}_{\mathcal{X}}$ on \mathcal{X} satisfies the inequality*

$$\overline{\omega}_{\mathcal{X}}^2 \leq (2g-2) \left([K : \mathbb{Q}] (\kappa_1 \log b_{\max} + \kappa_2) + \sum_{\mathfrak{p} \text{ bad}} a_{\mathfrak{p}} \log \text{Nm}(\mathfrak{p}) \right),$$

where κ_1, κ_2 are positive real constants that depend only on Y and the points ∞, P_1, \dots, P_r .

Proof: This follows from [Kü2, Theorem I] and (5.2). \square

The real number $\sum_{\mathfrak{p} \text{ bad}} a_{\mathfrak{p}} \log \text{Nm}(\mathfrak{p})$ is called the *geometric contribution*. Upper bounds for the geometric contribution which are easily computed from the configuration of the special fibers of \mathcal{X} can be found in [Kü2, §6]. The real number $[K : \mathbb{Q}] (\kappa_1 \log b_{\max} + \kappa_2)$ is called the *analytic contribution*.

5.3. Lower bounds. Let $S \in X(K)$ be a rational point with Zariski closure $\mathcal{S} \in \text{Div}(\mathcal{X})$ and let $V_S \in \text{Div}_{\mathbb{Q}}(\mathcal{X})$ denote a vertical \mathbb{Q} -divisor such that

$$(5.6) \quad (\mathcal{S} + V_S) \cdot \mathcal{C} = \frac{a_{\mathcal{C}}}{2g-2}$$

holds for all vertical irreducible components \mathcal{C} of \mathcal{X} , where $a_{\mathcal{C}}$ is defined in (2.3). Such a \mathbb{Q} -divisor exists by [KM, Proposition 2.1]. According to [KM, Corollary 2.3], we can also find, for every vertical irreducible component \mathcal{D} of \mathcal{X} , a vertical \mathbb{Q} -divisor $V_{\mathcal{D}} \in \text{Div}_{\mathbb{Q}}(\mathcal{X})$ such that

$$(V_{\mathcal{D}} \cdot \mathcal{C}) = \frac{a_{\mathcal{C}}}{2g-2} - \frac{\delta_{\mathcal{D}, \mathcal{C}}}{d_{\mathcal{D}}},$$

holds for all vertical irreducible components \mathcal{C} of \mathcal{X} , where $d_{\mathcal{D}}$ is the multiplicity of \mathcal{D} in the special fiber of \mathcal{X} containing it and δ is the Kronecker delta on the set of irreducible components. We set

$$U_S = \sum_{\mathcal{C}} d_{\mathcal{C}} (2(V_{\mathcal{C}} \cdot V_S) - V_{\mathcal{C}}^2) \mathcal{C}$$

and

$$\beta_S = \frac{1-g}{g} \overline{\mathcal{O}}(2V_S + U_S)^2 + 2(\overline{\omega}_{\mathcal{X}} \cdot \overline{\mathcal{O}}(U_S)),$$

where the vertical line bundles are equipped with the trivial metric. In [KM], Kühn and the second author used this to find a method for computing a lower bound for $\overline{\omega}_{\mathcal{X}}$.

Theorem 5.3. *With notation as above, suppose that*

- (i) $(2g-2)S$ is a canonical divisor on X ;
- (ii) we have

$$(5.7) \quad a_{\mathcal{C}} + 2(\mathcal{S} \cdot \mathcal{C}) - (U_S \cdot \mathcal{C}) \geq 0$$

for all vertical irreducible components \mathcal{C} of \mathcal{X} .

Then we have

$$\overline{\omega}_{\mathcal{X}}^2 \geq \beta_S.$$

Proof. See Proposition 1.2 and Theorem 1.3 of [KM]. \square

One can show that in favorable situations (for instance, when \mathcal{X} has only reduced special fibers and at least one of its special fibers is reducible), condition (i) can be dropped and condition (ii) is always satisfied and that β_S is a positive lower bound for $\bar{\omega}_{\mathcal{X}}^2$. However, For our intended application to $\mathcal{X} = \mathfrak{F}_N^{\min}$, we will have to check conditions (i) and (ii) and the positivity of β_S .

6. COMPUTATIONS ON THE LOCAL MINIMAL REGULAR MODEL

Let N be an odd squarefree natural number which has at least two prime factors, let ζ_N be a primitive N -th root of unity and let $F_N/\mathbb{Q}(\zeta_N)$ denote the Fermat curve (1.1). The minimal regular model \mathfrak{F}_N^{\min} of F_N over $\text{Spec } \mathbb{Z}_N$ was constructed in Part I. In order to bound $\omega_{\mathfrak{F}_N^{\min}}^2$ using Theorems 5.2 and 5.3 we need to show that these results are indeed applicable and we need to compute the quantities appearing in their statements. We recall the following notation from Section 3: Let $N = pm$, where p is prime and $m \in \mathbb{N}$. Fix a prime \mathfrak{p} of $\mathbb{Z}[\zeta_N]$ above p and let R be the localization of $\mathbb{Z}[\zeta_N]$ with respect to \mathfrak{p} . The minimal regular model $\mathfrak{F}_{N,\mathfrak{p}}^{\min} \rightarrow \text{Spec } R$ of the Fermat curve F_N over R is described explicitly in Theorem 3.13. We will mostly work on the base change $\mathfrak{F}_{N,\mathfrak{p}}^{\min} \times_{\text{Spec } R} \text{Spec } R^{sh}$, where R^{sh} is the strict Henselization of R . We denote the special fiber of this model by $\mathfrak{F}_{\pi} = \mathfrak{F}_{N,\mathfrak{p}}^{\min} \times_{\text{Spec } R} \text{Spec } \bar{\mathbb{F}}_p$.

6.1. Local extensions of cusps. Consider the Galois covering

$$(6.1) \quad \beta : F_N \rightarrow \mathbb{P}^1$$

of degree N^2 given by $(x : y : z) \mapsto (x^N : y^N)$. In fact β is a Belyi morphism, because it is unramified outside $0, 1, \infty$, and is defined over \mathbb{Q} with ramification orders all equal to N ; see [MR] for a discussion of the associated Belyi uniformization. In §7.1, we will use β to compute an upper bound on $\bar{\omega}_{\mathfrak{F}_N^{\min}}^2$ using Theorem 5.2. We call the ramification points of β the *cusps* of F_N . A divisor on X is called *cuspidal* if all points in its support are cuspidal. We now investigate the Zariski closures of the cusps inside the minimal regular model.

Notation 6.1. Assume that we have fixed a primitive N -th root of unity ζ_N . Then we denote by S_{x_i} (S_{y_i} , S_{z_i} , resp.) the cusp $(0 : \zeta_N^i : 1)$ ($(\zeta_N^i : 0 : 1)$, $(\zeta_N^i : -1 : 0)$, resp.). If the properties of the cusp, which are relevant for our consideration, do not depend on the exponent i we drop the subscript and just write S_x (S_y , S_z , resp.). For a normal model of the Fermat curve the Zariski closure of a cusp gives us a horizontal prime divisor. If there is no danger of confusion which normal model we consider we denote by \mathcal{S}_{x_i} , \mathcal{S}_x , \mathcal{S}_{y_i} , etc. the Zariski closure of S_{x_i} , S_x , S_{y_i} , etc.

Proposition 6.2. *Let S be a cusp of F_N and \mathcal{S} the horizontal divisor obtained by taking the Zariski closure of S in $\mathfrak{F}_{N,\mathfrak{p}}^{\min}$. Then \mathcal{S} only intersects one component of the geometric special fiber, namely one of the L_1 , see Figure 7. This intersection is transversal.*

Proof: We use Notation 6.1. By symmetry, we assume without loss of generality that $S = S_{x_i}$ for some i . If we take the Zariski closure of S in

$$\mathfrak{F}_{N,\mathfrak{p}}^0 = \text{Proj } R[X, Y, Z]/(X^N + Y^N - Z^N),$$

we get a horizontal divisor \mathcal{S}^0 which corresponds to the prime ideal $(X, Y - \zeta_N^i, Z - 1)$. It intersects the special fiber in the point $P_{x_i} = V_+((X, Y - \zeta_N^i, Z - 1, \pi))$. Now our minimal regular model $\mathfrak{F}_{N,p}^{min}$ comes with a birational morphism

$$(6.2) \quad f : \mathfrak{F}_{N,p}^{min} \rightarrow \mathfrak{F}_{N,p}^0;$$

in fact, f is just the composition of the blow-ups described in Proposition 3.5, Theorem 3.9 and Theorem 3.13. We have

$$(6.3) \quad \mathfrak{F}_{N,p}^{min} \times_{\text{Spec } R} \text{Spec } \overline{\mathbb{F}}_p \cdot \mathcal{S} = \deg_{K^{sh}} S = 1,$$

where $K^{sh} = \text{Frac}(R^{sh})$, see for instance [Liu, Remark 9.1.31]. It follows that

$$\mathfrak{F}_{N,p}^{min} \times_{\text{Spec } R} \text{Spec } \overline{\mathbb{F}}_p \cap \mathcal{S}$$

is reduced to a point P and that P belongs to a single irreducible component which is of multiplicity one, cf. [Liu, Corollary 9.1.32]. Furthermore, (6.3) shows that \mathcal{S} intersects this component transversally, see [Liu, Proposition 9.1.8]. On the other hand, we have $P \in f^{-1}(P_{x_i})$. But $f^{-1}(P_{x_i})$ consists of one component L_{XYZ} and p chains of components $L_1, L_2, \dots, L_{(m-1)}$, where a component $L_{(m-1)}$ intersect the component L_{XYZ} , cf. Figure 7. As the only components of $f^{-1}(P_{x_i})$ of multiplicity one are the L_1 's, P must lie on one of them. \square

Remark 6.3. In analogy with Proposition 6.2, the horizontal divisor that corresponds to a cusp S_{y_i} (S_{z_i} resp.) intersects a component L_1 that lies in $f^{-1}(P_{y_i})$ ($f^{-1}(P_{z_i})$ resp.), where $P_{y_i} = V_+((X - \zeta_N^i, Y, Z - 1, \pi))$ and $P_{z_i} = V_+((X - \zeta_N^i, Y + 1, Z, \pi))$, and no other component.

Since there are $3N$ components L_1 and $3N$ cusps it seems plausible that each L_1 is intersected by exactly one horizontal divisor which comes from a cusp. We show in the next proposition that this is indeed the case.

Proposition 6.4. *Let S and S' be cusps of F_N and denote by \mathcal{S} and \mathcal{S}' the associated horizontal divisors of $\mathfrak{F}_{N,p}^{min}$. Suppose that \mathcal{S} (\mathcal{S}' , resp.) intersects the component L (L' , resp.). Then we have $S = S'$ if and only if $L = L'$.*

Proof: It is clear that $L = L'$ if $S = S'$. Conversely, suppose that $S \neq S'$, but $L = L'$. According to Remark 6.3 we may assume without loss of generality that $S = S_{x_i}$ and $S' = S_{x_j}$ with $0 \leq j < i < N$. The morphism f in (6.2) factors as $f : \mathfrak{F}_{N,p}^{min} \xrightarrow{f_1} \mathfrak{F}_{N,p}^1 \xrightarrow{f_0} \mathfrak{F}_{N,p}^0$, where $\mathfrak{F}_{N,p}^1$ is the blow-up of $\mathfrak{F}_{N,p}^0$ along $V(X^m + Y^m - Z^m, \pi)$. The scheme $\mathfrak{F}_{N,p}^1$ is covered by $\tilde{\mathcal{X}}$ and $\tilde{\mathcal{X}}'$ (see the beginning of the proof of Theorem 3.13) and its special fiber consists of the components $F_m, L_{XYZ}, L_{\gamma_i}$ and L_δ . According to our assumption we must have $\text{Supp } f_1(\mathcal{S}_{x_i}) \cap \text{Supp } f_1(\mathcal{S}_{x_j}) = P$, where P is a closed point which lies in the special fiber of $\mathfrak{F}_{N,p}^1$; this follows because all the components L_i are blown down to points by f_1 . In fact P is a singular point which lies in the affine open subscheme $\tilde{\mathcal{X}}$ defined in Proposition 3.5. By (3.8) and the proof of Lemma 3.10, all singular points of $\tilde{\mathcal{X}}$ lie in $U_1 = \text{Spec } S_1$, so we can restrict our attention to this affine open subset. Because $F_m = W_1\pi$ in S_1 , an easy computation shows that

$$f_1(\mathcal{S}_{x_i})|_{U_1} = V\left(X, Y - \zeta_N^i, W_1 - \frac{(\zeta_N^{im} - 1)}{\pi}\right)$$

and

$$f_1(\mathcal{S}_{x_j})|_{U_1} = V\left(X, Y - \zeta_N^j, W_1 - \frac{(\zeta_N^{jm} - 1)}{\pi}\right)$$

(note that $\frac{(\zeta_N^{km}-1)}{\pi} \in R^*$ or $\frac{(\zeta_N^{km}-1)}{\pi} = 0$ since ζ_N^m is a primitive p -th root of unity). Let \mathfrak{m} be the maximal ideal of S_1 such that $V(\mathfrak{m}) = P$. Then

$$\zeta_N^i - \zeta_N^j = \zeta_N^j(\zeta_N^{i-j} - 1) \in \mathfrak{m}$$

and since $\pi \in \mathfrak{m}$, we must have $p \nmid i - j$. Indeed, let us assume that p divides $i - j$. Then the order of ζ_N^{i-j} is coprime to p and therefore \mathfrak{m} contains a natural number coprime to p , leading to a contradiction. On the other hand, since

$$\frac{(\zeta_N^{im} - 1)}{\pi} - \frac{(\zeta_N^{jm} - 1)}{\pi} = \frac{\zeta_N^{jm}(\zeta_N^{(i-j)m} - 1)}{\pi} \in \mathfrak{m},$$

we have $\zeta_N^{(i-j)m} = 1$, hence $p \mid i - j$. This gives us another contradiction and shows that $S = S'$. \square

6.2. Some vertical \mathbb{Q} -divisors and intersections. In this paragraph we define and study some \mathbb{Q} -divisors on $\mathfrak{F}_{N,p}^{min} \times_{\text{Spec } R} \text{Spec } R^{sh}$. These will be used to compute the geometric contribution in the upper bound given by Theorem 5.2 and the lower bound β_S in Theorem 5.3. The results are quite technical and the proofs consist mainly of straightforward, but lengthy calculations. Recall that \mathcal{T} denotes the set of irreducible components of the special fiber \mathfrak{F}_π and that

$$\mathfrak{F}_\pi = \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}} \mathcal{C},$$

where the components $\mathcal{C} \in \mathcal{T}$ and their multiplicities $d_{\mathcal{C}}$ are given in Figure 7 and Table 1.

Notation 6.5. We use the notation from Theorem 3.13. Let us fix a cusp S and a corresponding horizontal divisor \mathcal{S} . We know that \mathcal{S} intersects precisely one of the component of the special fiber; in fact it must be one of the components L_1 (Proposition 6.2). In the geometric special fiber \mathfrak{F}_π there are $3m$ components L_{XYZ} . To distinguish between these components we will number them and denote by $L^{(i)}$ the i -th one of the L_{XYZ} . Now for each component $L^{(i)}$ there are p chains of components $L_1, L_2, \dots, L_{(m-1)}$, where the $L_{(m-1)}$ intersect $L^{(i)}$. Again, we will number these chains. We denote the components of the chains by $L_{j,k}^{(i)}$, where the first subscript j indicates that it is one of the components L_j , the second subscript k means that it is a component of the k -th chain, and the superscript (i) indicates that the chain is attached to $L^{(i)}$. In the same way we proceed with the components L_γ and L_δ . We will number them and denote them by $L_\gamma^{(i)}$ and $L_\delta^{(i)}$. The components $L_{\gamma,j}$ will be denoted by $L_{\gamma,j}^{(i)}$, where the superscript i indicates that $L_{\gamma,j}^{(i)}$ intersects $L_\gamma^{(i)}$. Without loss of generality we assume that we fixed this numbering so that \mathcal{S} intersects the component $L_{1,1}^{(1)}$.

We now define the following vertical \mathbb{Q} -divisors on \mathfrak{F}_π :

$$\begin{aligned}
V_{F_m} &= \frac{p-2}{2g-2} F_m \\
V_{L_\delta^{(i)}} &= V_{F_m} + \frac{1}{p} L_\delta^{(i)}, \quad 1 \leq i \leq m^2(p-3) - 2m\varrho \\
V_{L_\gamma^{(i)}} &= V_{F_m} + \frac{1}{p} L_\gamma^{(i)} + \sum_{j=1}^p \frac{1}{2p} L_{\gamma,j}^{(i)}, \quad 1 \leq i \leq m\varrho \\
V_{L_{\gamma,s}^{(i)}} &= V_{F_m} + \frac{1}{p} L_\gamma^{(i)} + \sum_{j=1}^p \frac{1}{2p} L_{\gamma,j}^{(i)} + \frac{1}{2} L_{\gamma,s}^{(i)}, \quad 1 \leq i \leq m\varrho, 1 \leq s \leq p \\
V_{L^{(i)}} &= V_{F_m} + \frac{1}{p} L^{(i)} + \sum_{j=1}^{m-1} \sum_{k=1}^p \frac{j}{N} L_{j,k}^{(i)}, \quad 1 \leq i \leq 3m \\
V_{L_{r,s}^{(i)}} &= V_{F_m} + \frac{r}{p} L^{(i)} + \sum_{j=1}^{m-1} \sum_{k=1}^p \frac{jr}{N} L_{j,k}^{(i)} + \sum_{j=1}^{r-1} \frac{j(m-r)}{m} L_{j,s}^{(i)} \\
&\quad + \sum_{j=r}^{m-1} \frac{r(m-j)}{m} L_{j,s}^{(i)}, \quad 1 \leq i \leq 3m, 1 \leq r \leq m-1, 1 \leq s \leq p
\end{aligned}$$

Recall that if \mathcal{C} is an irreducible component of \mathfrak{F}_π , then we have $a_{\mathcal{C}} = (\mathcal{K} \cdot \mathcal{C})$ by the adjunction formula (Theorem 2.17), where $a_{\mathcal{C}} = -\mathcal{C}^2 + 2p_a(\mathcal{C}) - 2$ and \mathcal{K} is a canonical \mathbb{Q} -divisor of $\mathfrak{F}_{N,p}^{\min} \times_{\text{Spec}(R)} \text{Spec}(R^{sh})$.

Lemma 6.6. *Let $\mathcal{D} \in \mathcal{T}$ be an irreducible component of \mathfrak{F}_π . Then we have*

$$(V_{\mathcal{D}} \cdot \mathcal{C}) = \frac{a_{\mathcal{C}}}{2g-2} - \frac{\delta_{\mathcal{D},\mathcal{C}}}{d_{\mathcal{C}}}$$

for all $\mathcal{C} \in \mathcal{T}$, where δ is the Kronecker delta on \mathcal{T} .

Proof. This can be verified by a straightforward computation using Theorem 3.13. \square

Next we compute the self-intersections of the \mathbb{Q} -divisors $V_{\mathcal{D}}$. Let us denote

$$\lambda = -\left(\frac{m(p-2)}{2(g-1)}\right)^2 \quad \text{and} \quad \nu = \frac{p-2}{p(g-1)}.$$

Lemma 6.7. *We have*

$$\begin{aligned}
V_{F_m}^2 &= \lambda \\
V_{L_\delta^{(i)}}^2 &= \lambda + \nu - \frac{1}{p} \\
V_{L_\gamma^{(i)}}^2 &= \lambda + \nu - \frac{1}{2p} \\
V_{L_{\gamma,s}^{(i)}}^2 &= \lambda + \nu - \frac{1+p}{2p} \\
V_{L^{(i)}}^2 &= \lambda + \nu - \frac{1}{N} \\
V_{L_{r,s}^{(i)}}^2 &= \lambda + r\nu - \frac{r+N-rp}{N}.
\end{aligned}$$

Proof. We obviously have $V_{F_m}^2 = \lambda$. For the other components $\mathcal{D} \in \mathcal{T}$, we can write $V_{\mathcal{D}} = V_{F_m} + W_{\mathcal{D}}$ and compute

$$V_{\mathcal{D}}^2 = \lambda + W_{\mathcal{D}}^2 + p\nu(F_m \cdot W_{\mathcal{D}}).$$

Alternatively, we can write $V_{\mathcal{D}} = \sum_{\mathcal{C} \in \mathcal{T}} r_{\mathcal{C}} \mathcal{C}$ and use Lemma 6.6, which implies

$$(6.4) \quad V_{\mathcal{D}}^2 = \left(V_{\mathcal{D}} \cdot \sum_{\mathcal{C} \in \mathcal{T}} r_{\mathcal{C}} \mathcal{C} \right) = \sum_{\mathcal{C} \in \mathcal{T}} r_{\mathcal{C}} \left(\frac{a_{\mathcal{C}}}{2g-2} - \frac{\delta_{\mathcal{D}\mathcal{C}}}{d_{\mathcal{C}}} \right).$$

Either one of these formulas leads to a straightforward proof of the assertion. \square

Recall that we have fixed a cusp S whose Zariski closure \mathcal{S} in $\mathfrak{F}_{N,p}^{min}$ intersects the component $L_{1,1}^{(1)}$, and no other $\mathcal{C} \in \mathcal{T}$. Setting

$$(6.5) \quad V_{S,p} = V_S = V_{L_{1,1}^{(1)}},$$

Lemma 6.6 implies

$$(6.6) \quad (\mathcal{S} + V_S) \cdot \mathcal{C} = \frac{a_{\mathcal{C}}}{2g-2}$$

for all $\mathcal{C} \in \mathcal{T}$. Note that we have

$$(6.7) \quad V_S = 2p\nu F_m + \frac{1}{p} L^{(1)} + \sum_{j=1}^{m-1} \sum_{k=1}^p \mu_{j,k} L_{j,k}^{(1)},$$

where

$$\mu_{j,1} = \frac{j - jp + N}{N} \quad \text{and} \quad \mu_{j,k} = \frac{j}{N} \text{ for } k \neq 1.$$

The \mathbb{Q} -divisor V_S will play a crucial part in Section 7. On the one hand, it will be used to construct the divisors \mathcal{F}_j (defined in (5.3)) whose self-intersections appear in Theorem 5.2. On the other hand, the lower bound β_S from Theorem 5.3 is defined using V_S .

We start by analyzing the intersections of V_S with the \mathbb{Q} -divisors $V_{\mathcal{C}}$ for $\mathcal{C} \in \mathcal{T}$.

Lemma 6.8. *We have*

$$\begin{aligned} (V_S \cdot V_{F_m}) &= \lambda + \frac{1}{2}\nu \\ (V_S \cdot V_{L_{\delta}^{(i)}}) &= \lambda + \nu \\ (V_S \cdot V_{L_{\gamma}^{(i)}}) &= \lambda + \nu \\ (V_S \cdot V_{L_{\gamma,s}^{(i)}}) &= \lambda + \nu \\ (V_S \cdot V_{L^{(i)}}) &= \lambda + \nu - \frac{\delta_{1i}}{N} \\ (V_S \cdot V_{L_{r,s}^{(i)}}) &= \lambda + \frac{r+1}{2}\nu - \frac{r\delta_{1i}}{N} - \frac{(m-u)\delta_{1i}\delta_{1s}}{m}, \end{aligned}$$

where δ is the Kronecker delta on $\{1, \dots, 3m\}$.

Proof. The proof is similar to the proof of Lemma 6.7. Namely, if $V_{\mathcal{D}} = \sum_{\mathcal{C} \in \mathcal{T}} r_{\mathcal{C}} \mathcal{C}$, then Lemma 6.6 implies

$$(V_S \cdot V_{\mathcal{D}}) = \sum_{\mathcal{C} \in \mathcal{T}} r_{\mathcal{C}} \left(\frac{a_{\mathcal{C}}}{2g-2} - \frac{\delta_{L_{1,1}^{(1)}, \mathcal{C}}}{d_{\mathcal{C}}} \right).$$

Using this, the proof consists of elementary computations. \square

We now use the vertical \mathbb{Q} -divisors $V_{\mathcal{C}}$ to define another vertical \mathbb{Q} -divisor

$$U_{S,\mathfrak{p}} = U_S = \sum_{\mathcal{C} \in \mathcal{T}} d_{\mathcal{C}} (2(V_{\mathcal{C}} \cdot V_S) - V_S^2) \mathcal{C} - (\lambda + \mu) \mathfrak{F}_{\pi}.$$

Lemma 6.9. *We have*

$$\begin{aligned} U_S = & \sum_{i=1}^{m^2(p-3)-2m\varrho} \frac{1}{p} L_{\delta}^{(i)} + \sum_{i=1}^{m\varrho} \frac{1}{p} L_{\gamma}^{(i)} + \sum_{i=1}^{m\varrho} \sum_{j=1}^p \frac{1+p}{p} L_{\gamma,j}^{(i)} + \sum_{i=1}^{3m} \frac{1}{p} L^{(i)} - \frac{2}{p} L^{(1)} \\ & + \sum_{i=1}^{3m} \sum_{j=1}^{m-1} \sum_{k=1}^p j \mu_{j,1} L_{j,k}^{(i)} - \sum_{j=1}^{m-1} \sum_{k=1}^p \frac{2j}{N} L_{j,k}^{(1)} - \sum_{j=1}^{m-1} \frac{2(m-j)}{m} L_{j,1}^{(1)}. \end{aligned}$$

Proof. This is a simple computation using Lemma 6.7 and Lemma 6.8. \square

As a corollary, we get the following result on the intersection multiplicities between U_S and the components $\mathcal{C} \in \mathcal{T}$.

Lemma 6.10. *If \mathcal{C} is an irreducible component of \mathfrak{F}_{π} , then we have*

$$a_{\mathcal{C}} + 2(\mathcal{S} \cdot \mathcal{C}) - (U_S \cdot \mathcal{C}) \geq 0.$$

Proof. We only show the claim for $\mathcal{C} = L_{\delta}^{(i)}$. Using Lemma 6.9, we find

$$(U_S \cdot L_{\delta}^{(i)}) = \frac{1}{p} (L_{\delta}^{(i)})^2 = -1$$

and hence

$$a_{L_{\delta}^{(i)}} + (\mathcal{S} \cdot L_{\delta}^{(i)}) - (U_S \cdot L_{\delta}^{(i)}) = p - 1 \geq 0.$$

The other cases are similar and are left to the reader. \square

Let us define

$$\beta_{S,\mathfrak{p}} = \beta_S = \frac{1-g}{g} (2V_S + U_S)^2 + 2(\mathcal{K} \cdot U_S),$$

where \mathcal{K} is a canonical \mathbb{Q} -divisor of $\mathfrak{F}_{N,\mathfrak{p}}^{\min} \times_{\text{Spec}(R)} \text{Spec}(R^{sh})$. Summing up all $\beta_{S,\mathfrak{p}}$ as \mathfrak{p} runs through the bad primes of \mathcal{O}_K , we will get a lower bound for $\bar{\omega}_{\mathfrak{F}_N}^2$ in §7.2 using Theorem 5.3.

Proposition 6.11. *We have*

$$\beta_S = N(\lambda + \nu) \left(\frac{N(\lambda + \nu)(g-1)}{g} + 4m - 6 \right).$$

Proof. Applying Lemma 6.9, we see that

$$\begin{aligned} 2V_S + U_S = & \sum_{i=1}^{m^2(p-3)-2m\varrho} \frac{1}{p} L_{\delta}^{(i)} + \sum_{i=1}^{m\varrho} \frac{1}{p} L_{\gamma}^{(i)} + \sum_{i=1}^{m\varrho} \sum_{j=1}^p \frac{1+p}{p} L_{\gamma,j}^{(i)} + \sum_{i=1}^{3m} \frac{1}{p} L_{XYZ}^{(i)} \\ & + \sum_{i=1}^{3m} \sum_{j=1}^{m-1} \sum_{k=1}^p \mu_{j,1} L_{j,k}^{(i)}. \end{aligned}$$

A simple computation shows

$$(6.8) \quad (2V_S + U_S)^2 = -(N(\lambda + \nu))^2.$$

Using the adjunction formula, it is easy to see that

$$(6.9) \quad (\mathcal{K} \cdot U_S) = (2m-3)N(\lambda + \nu).$$

The result follows from (6.8) and (6.9). \square

Remark 6.12. Suppose that S is a cusp whose Zariski closure \mathcal{S} intersects $L_{1,k}^{(i)}$, where $(i, k) \neq (1, 1)$. Then Lemma 6.10 and Proposition 6.11 remain valid (with the obvious index modifications); the proofs are entirely analogous.

It remains to compute local versions of the divisors \mathcal{G}_j , defined in (5.4). By Theorem 5.2, these are needed for the upper bound for $\bar{\omega}_{\mathfrak{F}_N}^2$. As $\mathfrak{F}_{N,p}^{min}$ is constructed using a sequence of blow-ups, the morphism $\beta : F_N \rightarrow \mathbb{P}^1$ in (6.1) extends to a morphism

$$\beta : \mathfrak{F}_{N,p}^{min} \rightarrow \mathbb{P}_R^1.$$

For our applications (see Section 7) we need to construct a divisor of $\mathfrak{F}_{N,p}^{min}$ whose associated line bundle is isomorphic to the pullback of the twist $\mathcal{O}_{\mathbb{P}_R^1}(1)$ by β .

We set

$$(6.10) \quad \mathcal{G}_{S,p} = \mathcal{G}_S = \sum_{j=1}^{m-1} \sum_{k=1}^p \mu_{j,k} L_{j,k}^{(1)} + \mu L_{1,1}^{(1)},$$

Lemma 6.13. *Let*

$$\mathcal{E}_S = \mathcal{S} + \mathcal{G}_S,$$

where \mathcal{G}_S is the vertical \mathbb{Q} -divisor in (6.10). Then \mathcal{E}_S is a \mathbb{Q} -divisor of $\mathfrak{F}_{N,p}^{min}$ which is associated to $(\beta^ \mathcal{O}_{\mathbb{P}_R^1}(1))^{\otimes \frac{1}{N^2}}$.*

Proof: We can show that $N^2 \mathcal{S}$ is associated to $\beta^* \mathcal{O}_{\mathbb{P}_K^1}(1)$, where K is the fraction field of R , using arguments analogous to those employed in [CK, Lemma 7.3]. Since

$$\beta^* \mathcal{O}_{\mathbb{P}_R^1}(1)|_{F_N} \cong \beta^* \mathcal{O}_{\mathbb{P}_K^1}(1),$$

it is clear that there is a \mathbb{Q} -divisor of the form $\mathcal{E}_S = \mathcal{S} + \mathcal{G}_S$, with a vertical \mathbb{Q} -divisor \mathcal{G}_S , such that \mathcal{E}_S is associated to $(\beta^* \mathcal{O}_{\mathbb{P}_R^1}(1))^{\otimes \frac{1}{N^2}}$. The \mathbb{Q} -divisor \mathcal{E}_S has to satisfy the equations

$$(6.11) \quad (N^2 \mathcal{E}_S \cdot \mathcal{C}) = 0$$

for all components \mathcal{C} which are different from F_m (see e.g. [Liu, Theorem 9.2.12]), and

$$(6.12) \quad N^2 = (N^2 \mathcal{E}_S \cdot \mathfrak{F}_{N,p}^{min} \times_{\text{Spec } R} \text{Spec } \mathbb{F}_p) = (N^2 \mathcal{E}_S \cdot p F_m),$$

see [Liu, Remark 9.1.131]. One can use the quantities computed in Theorem 3.13 to verify that our choice of \mathcal{G}_S in (6.10) indeed satisfies the equations (6.11) and (6.12). \square

Proposition 6.14. *We have*

$$\mathcal{G}_S^2 = -\frac{N - p + 1}{N}.$$

Proof: Note that by (6.7), we have $\mathcal{G}_S = V_S - V_{F_m}$. Thus the result follows from Lemma 6.7 and Lemma 6.8. \square

Remark 6.15. Suppose that S is a cusp whose Zariski closure \mathcal{S} intersects $L_{1,k}^{(i)}$, where $(i, k) \neq (1, 1)$. Then analogues of Lemma 6.13 and Proposition 6.14 for S can be proved in an similar way.

7. BOUNDS FOR $\bar{\omega}_{\mathfrak{F}_N^{min}}^2$

In this section we compute upper and lower bounds for the arithmetic self-intersection $\bar{\omega}_{\mathfrak{F}_N^{min}}^2$ of the dualizing sheaf on the minimal regular model \mathfrak{F}_N^{min} over $\text{Spec}(\mathbb{Z}_N)$ of the Fermat curve F_N .

7.1. An upper bound for $\bar{\omega}_{\mathfrak{F}_N^{min}}^2$. We want to apply Theorem 5.2 to find an upper bound for $\bar{\omega}_{\mathfrak{F}_N^{min}}^2$. The morphism $\beta : F_N \rightarrow \mathbb{P}^1$ from (6.1) is unramified outside $0, 1, \infty$ and extends to a morphism

$$\beta : \mathfrak{F}_N^{min} \rightarrow \mathbb{P}_{\mathbb{Z}[\zeta_N]}^1,$$

since the minimal regular model \mathfrak{F}_N^{min} can be constructed by a sequence of blow-ups, see Section 3. We will apply Theorem 5.2 with $\beta : \mathfrak{F}_N^{min} \rightarrow \mathbb{P}_{\mathbb{Z}[\zeta_N]}^1$. To compute the geometric contribution, we construct \mathbb{Q} -divisors \mathcal{F}_j and \mathcal{G}_j as in Section 5.2, using the local results from §6.2. Recall that the cusps on F_N are the points which are mapped to $0, 1$ or ∞ by β and that a divisor on F_N is called cuspidal if its support consists entirely of cusps.

We first construct the \mathbb{Q} -divisors \mathcal{F}_j .

Theorem 7.1 (Rohrlich). *The group of cuspidal divisors on F_N modulo the group of principal cuspidal divisors is a torsion group.*

Proof: The statement follows from [Ro, Theorem 1]. □

Corollary 7.2. *Let $S \in F_N(\mathbb{Q}(\zeta_N))$ be a cusp. Then $(2g - 2)S$ is a canonical divisor.*

Proof: The corollary follows from Theorem 7.1, because the Hurwitz formula implies that there exists a canonical divisor with support in the cusps. □

Proposition 7.3. *Let $S_j \in F_N$ be a cusp and let $\mathcal{S}_j \in \text{Div}(\mathfrak{F}_N^{min})$ be its Zariski closure. Set*

$$\mathcal{F}_j = \sum_{\mathfrak{p} \text{ bad}} V_{S_j, \mathfrak{p}},$$

where $V_{S_j, \mathfrak{p}}$ is the vertical \mathbb{Q} -divisor supported in the special fiber above \mathfrak{p} defined in (6.5), viewed as a \mathbb{Q} -divisor on \mathfrak{F}_N^{min} . Then

- (i) $(2g - 2)(\mathcal{S}_j + \mathcal{F}_j)$ is a canonical \mathbb{Q} -divisor on \mathfrak{F}_N^{min} ;
- (ii) \mathcal{F}_j satisfies (5.3).

Proof. It is clear that (ii) follows from (i). By Corollary 7.2, the divisor $(2g - 2)S_j$ is a canonical divisor on F_N . Hence, by [CK, Proposition 2.5], a \mathbb{Q} -divisor \mathcal{K} on \mathfrak{F}_N^{min} of the form

$$\mathcal{K} = (2g - 2)\mathcal{S}_j + \mathcal{V},$$

where \mathcal{V} is a vertical \mathbb{Q} -divisor, is canonical if and only if \mathcal{K} satisfies the adjunction formula (Theorem 2.17). By (6.6), the \mathbb{Q} -divisor

$$\mathcal{K} = (2g - 2)(\mathcal{S}_j + \mathcal{F}_j)$$

satisfies the adjunction formula, so (i) follows. □

We now find, for cusps S_j above ∞ , \mathbb{Q} -divisors \mathcal{G}_j such that (5.4) is satisfied. To this end, we use the vertical \mathbb{Q} -divisors $\mathcal{G}_{S_j, \mathfrak{p}}$, see (6.10) and Remark 6.15.

Lemma 7.4. *Let $S_j \in F_N$ be a cusp above ∞ with Zariski closure $\mathcal{S}_j \in \text{Div}(\mathfrak{F}_N^{\min})$. Then the \mathbb{Q} -divisor*

$$\mathcal{E}_{S_j} = \mathcal{S}_j + \sum_{\mathfrak{p} \text{ bad}} \mathcal{G}_{S_j, \mathfrak{p}}$$

is associated with $(\beta^ \mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_N]}}(1))^{\otimes \frac{1}{N^2}}$, where we view each $\mathcal{G}_{S_j, \mathfrak{p}}$ as a \mathbb{Q} -divisor on \mathfrak{F}_N^{\min} .*

Proof: We can assume that the \mathbb{Q} -divisor we are looking for is of the form $\mathcal{E}_{S_j} = \mathcal{S}_j + \mathcal{G}$, where \mathcal{G} is a vertical \mathbb{Q} -divisor with support in the bad fibers. If \mathfrak{p} is a prime of bad reduction above p and \mathcal{C} is an irreducible component of the special fiber above \mathfrak{p} which is different from the component $F_{N/p}$, then the \mathbb{Q} -divisor \mathcal{E}_{S_j} has to satisfy

$$(N^2 \mathcal{E}_{S_j} \cdot \mathcal{C}) = 0.$$

Furthermore, \mathcal{E}_{S_j} has to satisfy

$$N^2 = (N^2 \mathcal{E}_{S_j} \cdot \mathfrak{F}_N^{\min} \times_{\text{Spec } \mathbb{Z}[\zeta_N]} \text{Spec } \mathbb{F}_p) = (N^2 \mathcal{E}_{S_j} \cdot p F_{N/p}).$$

On the other hand, if we take $\mathcal{G} = \sum_{\mathfrak{p} \text{ bad}} \mathcal{G}_{S_j, \mathfrak{p}}$, then these equations are satisfied, because a component \mathcal{C} which belongs to the fiber above \mathfrak{p} only intersects $\mathcal{G}_{S_j, \mathfrak{p}}$. It follows that our choice of \mathcal{G} is valid. \square

Corollary 7.5. *Let S_j be a cusp which lies above the branch point ∞ . Let us set*

$$\mathcal{G}_j = \sum_{\mathfrak{p} \text{ bad}} \mathcal{G}_{S_j, \mathfrak{p}}.$$

Then \mathcal{G}_j satisfies (5.4).

Proof: The Zariski closure $\overline{\infty}$ of ∞ in $\mathbb{P}^1_{\mathbb{Z}[\zeta_N]}$ is associated to $\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_N]}}(1)$. Because S_j lies above the branch point ∞ , Lemma 7.4 implies that (5.4) is satisfied for the section $s = \beta^*(1) \in \beta^* \mathcal{O}(\infty)$. \square

Lemma 7.6. *Let S_j be a cusp above ∞ , let $p|N$ be a prime and let \mathfrak{p} be a prime above p . Then the self-intersections $V_{S_j, p}^2 := V_{S_j, \mathfrak{p}}^2$ and $\mathcal{G}_p^2 := \mathcal{G}_{S_j, \mathfrak{p}}^2$ are independent of \mathfrak{p} . Furthermore, we have*

$$\overline{\mathcal{O}}(\mathcal{F}_j)^2 = \sum_{p|N} \varphi(N)/\varphi(p) V_{S_j, p}^2 \log p$$

and

$$\overline{\mathcal{O}}(\mathcal{G}_j)^2 = \sum_{p|N} \varphi(N)/\varphi(p) \mathcal{G}_{S_j, p}^2 \log p,$$

Proof: For prime ideals of $\mathbb{Z}[\zeta_N]$ above the same prime number p , the corresponding special fibers of \mathfrak{F}_N^{\min} are isomorphic, proving the first statement.

We have

$$\overline{\mathcal{O}}(\mathcal{F}_j)^2 = \sum_{\mathfrak{p} \text{ bad}} \overline{\mathcal{O}}(V_{S_j, \mathfrak{p}})^2 = \sum_{p|N} \sum_{\substack{\mathfrak{p} \text{ bad} \\ \mathfrak{p} \cap \mathbb{Z} = (p)}} \overline{\mathcal{O}}(V_{S_j, \mathfrak{p}})^2,$$

with $\overline{\mathcal{O}}(V_{S_j, \mathfrak{p}})^2 = \mathcal{F}_p^2 \log \text{Nm}(\mathfrak{p})$ by (5.1). For each prime p let us denote by r_p the number of prime ideals of $\mathbb{Z}[\zeta_N]$ that lie above p . Since $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is a Galois extension, all the inertia degrees and ramification indices of the prime ideals over p are the same (we denote

them by f_p and e_p , respectively), and we get the equation $\varphi(N) = [\mathbb{Q}(\zeta_N) : \mathbb{Q}] = e_p f_p r_p$. Because $e_p = \varphi(p)$, we have

$$r_p \log \text{Nm}(\mathfrak{p}) = \varphi(N)/\varphi(p) \log(p)$$

for a prime ideal \mathfrak{p} above p . Hence it follows that

$$\sum_{\substack{\mathfrak{p} \text{ bad} \\ \mathfrak{p} \cap \mathbb{Z} = (p)}} \overline{\mathcal{O}}(V_{S_j, \mathfrak{p}})^2 = r_p V_{S_j, \mathfrak{p}}^2 \log \text{Nm}(\mathfrak{p}) = \varphi(N)/\varphi(p) V_{S_j, \mathfrak{p}}^2 \log p.$$

Summing up over all prime numbers p with $p|N$, we obtain the formula for $\overline{\mathcal{O}}(\mathcal{F}_j)^2$. The claimed formula for $\overline{\mathcal{O}}(\mathcal{G}_j)^2$ can be verified in a similar way. \square

We now prove the main result of this section.

Theorem 7.7. *Let $N > 0$ be an odd squarefree integer with at least two prime factors, and let \mathfrak{F}_N^{\min} be the minimal regular model of the Fermat curve F_N over $\text{Spec } \mathbb{Z}[\zeta_N]$. Then the arithmetic self-intersection number of its dualizing sheaf equipped with the Arakelov metric satisfies*

$$\begin{aligned} \overline{\omega}_{\mathfrak{F}_N^{\min}}^2 &\leq (2g - 2)[\mathbb{Q}(\zeta_N) : \mathbb{Q}](\kappa_1 \log N + \kappa_2) \\ &\quad + (2g - 2) \sum_{p|N} \frac{\varphi(N)}{\varphi(p)} \left(\frac{3N^2 - 2Np - 10N + 6p - 6 - 4\left(\frac{N}{p}\right)^2 + 12\left(\frac{N}{p}\right)}{N(N - 3)} \right) \log p, \end{aligned}$$

where $\kappa_1, \kappa_2 \in \mathbb{R}$ are positive constants independent of N .

Proof: The morphism $\beta : \mathfrak{F}_N^{\min} \rightarrow \mathbb{P}_{\mathbb{Z}[\zeta_N]}^1$ is a morphism of arithmetic surfaces which satisfies the requirements of Theorem 5.2. We have $\deg \beta = N^2$ and $\beta^* \infty = \sum_{j=1}^N NS_j$, hence $b_j = b_{\max} = N$. It follows that in our case the formula (5.5) of Theorem 5.2 becomes

$$\begin{aligned} \sum_{\mathfrak{p} \text{ bad}} a_{\mathfrak{p}} \log \text{Nm}(\mathfrak{p}) &= -2g \overline{\mathcal{O}}(\mathcal{G}_j)^2 + (2g - 2) \overline{\mathcal{O}}(\mathcal{F}_j)^2 \\ &= \sum_{p|N} \frac{\varphi(N)}{\varphi(p)} \left(-2g \mathcal{G}_{S_j, p}^2 + (2g - 2) V_{S_j, p}^2 \right) \log p \\ &= \sum_{p|N} \frac{\varphi(N)}{\varphi(p)} \left(\frac{3N^2 - 2Np - 10N + 6p - 6 - 4\left(\frac{N}{p}\right)^2 + 12\left(\frac{N}{p}\right)}{N(N - 3)} \right) \log p, \end{aligned}$$

where we used Lemma 7.6 for the second equality. The final equality follows from Lemma 6.7 and Proposition 6.14. \square

For the proof of Theorem 1.1 from the introduction, we also need the following simple fact.

Lemma 7.8. *We have*

$$\sum_{p|N} \frac{\log p}{p - 1} \leq \mathcal{O}(\log \log N)$$

for $N \in \mathbb{N}$ odd and squarefree.

Proof. We bound $\sum_{1 < n \leq x} \frac{\log p_n}{p_n - 1}$, where p_n is the n -th prime. It is well known that

$$n \log n < p_n < n \log n + n \log \log n,$$

for $n \geq 6$, so

$$\frac{\log p_n}{p_n - 1} < \frac{\log n}{n \log n - 1} + \frac{\log(\log n + \log \log n)}{n \log n - 1} \leq \frac{4}{n}.$$

follows for $n \geq 6$, implying

$$\sum_{1 < n \leq x} \frac{\log p_n}{p_n - 1} \leq 4 \log x + c,$$

where c is a constant independent of x . Now the number of prime divisors of N is of order $\mathcal{O}(\log N / \log \log N)$ by [HW, Chapter 22], so the result follows. \square

We can now deduce Theorem 1.1 from Theorem 7.7 and Lemma 7.8.

Proof of Theorem 1.1: We have

$$\begin{aligned} \sum_{\mathfrak{p} \text{ bad}} a_{\mathfrak{p}} \log \text{Nm}(\mathfrak{p}) &= \sum_{p|N} \frac{\varphi(N)}{\varphi(p)} \left(\frac{3N^2 - 2Np - 10N + 6p - 6 - 4\left(\frac{N}{p}\right)^2 + 12\left(\frac{N}{p}\right)}{N(N-3)} \right) \log p \\ &\leq \sum_{p|N} \frac{\varphi(N)}{\varphi(p)} \frac{3N}{N-3} \log p \leq \frac{15}{4} \varphi(N) \sum_{p|N} \frac{\log p}{p-1} = \varphi(N) \mathcal{O}(\log \log N) \end{aligned}$$

for the geometric contribution by Lemma 7.8.

The analytic contribution is

$$\varphi(N)(\kappa_1 \log N + \kappa_2) = \varphi(N)\kappa_1 \log N + \mathcal{O}(\varphi(N)).$$

Setting $\kappa = \kappa_1$, we find

$$\bar{\omega}_{\mathfrak{F}_N}^2 \leq (2g - 2)\kappa\varphi(N) \log N + \mathcal{O}(g\varphi(N) \log \log N),$$

which is the statement of Theorem 1.1. \square

7.2. A lower bound for $\bar{\omega}_{\mathfrak{F}_N}^2$. In order to use Theorem 5.3 to obtain a lower bound for $\bar{\omega}_{\mathfrak{F}_N}^2$, we need to find a suitable rational point $S \in F_N(\mathbb{Q}(\zeta_N))$ such that properties (i) and (ii) of Theorem 5.3 are satisfied.

Let S be one of the cusps of F_N . We use the notation of Section 5.3. Recall that, for a prime $\mathfrak{p}|N$ of $\mathbb{Z}[\zeta_N]$, we defined vertical \mathbb{Q} -divisors $V_{S,\mathfrak{p}}$ and $U_{S,\mathfrak{p}}$, and gave a formula for

$$\beta_{S,\mathfrak{p}} = \frac{1-g}{g} (2V_{S,\mathfrak{p}} + U_{S,\mathfrak{p}})^2 + 2(\mathcal{K}_{\mathfrak{p}} \cdot U_{S,\mathfrak{p}})$$

in Proposition 6.11, where $\mathcal{K}_{\mathfrak{p}}$ is a canonical \mathbb{Q} -divisor on $\mathfrak{F}_{N,\mathfrak{p}}^{\min}$.

Lemma 7.9. *For a prime $p|N$ and a prime \mathfrak{p} above p , the numbers $\beta_{S,p} := \beta_{S,\mathfrak{p}}$ are independent of \mathfrak{p} . Furthermore, we have*

$$\beta_S = \sum_{p|N} \frac{\varphi(N)}{\varphi(p)} \beta_{S,p} \log p.$$

Proof: Since all special fibers above primes dividing a prime number p are isomorphic, the first statement follows.

To prove the second statement, note that

$$V_S = \sum_{p|N} \sum_{\substack{\mathfrak{p} \text{ bad} \\ \mathfrak{p} \cap \mathbb{Z} = (p)}} V_{S,\mathfrak{p}}$$

satisfies (5.6) and that we have

$$U_S = \sum_{p|N} \sum_{\substack{\mathfrak{p} \text{ bad} \\ \mathfrak{p} \cap \mathbb{Z} = (p)}} U_{S,\mathfrak{p}},$$

yielding

$$\beta_S = \sum_{p|N} \sum_{\substack{\mathfrak{p} \text{ bad} \\ \mathfrak{p} \cap \mathbb{Z} = (p)}} \beta_{S,\mathfrak{p}} \log \text{Nm}(\mathfrak{p}).$$

Now the second statement follows as in the proof of Lemma 7.6. \square

We now prove the main result of this section.

Theorem 7.10. *Let $N > 0$ be an odd squarefree integer with at least two prime factors, and let \mathfrak{F}_N^{\min} be the minimal regular model of the Fermat curve F_N over $\text{Spec } \mathbb{Z}[\zeta_N]$. Then we have*

$$\bar{\omega}_{\mathfrak{F}_N^{\min}}^2 \geq \varphi(N) \sum_{p|N} \frac{\alpha(N, p)(Np + 2N - 6p)(p - 2)}{(N - 1)(N - 2)(N - 3)^3 p^4 (p - 1)} \log p,$$

where

$$\alpha(N, p) = 4N^4 p - 6N^3 p^2 - 24N^3 p + 37N^2 p^2 + 44N^2 p - 72N p^2 - 4N^2 - 12N p + 36p^2.$$

Proof. Corollary 7.2 implies that $(2g - 2)S$ is a canonical divisor on F_N . By Lemma 6.10, we see that (5.7) is satisfied for all irreducible vertical components, so that Theorem 5.3 is applicable. Therefore we obtain the lower bound

$$\bar{\omega}_{\mathfrak{F}_N^{\min}}^2 \geq \sum_{p|N} \frac{\varphi(N)}{\varphi(p)} \beta_{S,p} \log p$$

from Lemma 7.9. By Proposition 6.11, we have

$$\beta_{S,p} = \frac{\alpha(N, p)(Np + 2N - 6p)(p - 2)}{(N - 1)(N - 2)(N - 3)^3 p^4},$$

which proves the result. \square

Proof of Theorem 1.2. Let N be odd, composite and squarefree and let p be a prime dividing N . From $p \leq \frac{N}{3}$ we get

$$Np + 2N - 6p \geq Np.$$

Moreover, using $N \geq 15$ we find

$$\begin{aligned} \alpha(N, p) &= (4N^4 p - 6N^3 p^2 - 24N^3 p) + (37N^2 p^2 + 44N^2 p - 72N p^2 - 4N^2 - 12N p + 36p^2) \\ &\geq 2N^3 p(2N - 3p - 12) + N(37N p^2 + 20N p - 4N - 12p) \\ &\geq \frac{2}{5} N^4 p + 43N^2 p^2, \end{aligned}$$

where $\alpha(N, p)$ is as in Theorem 7.10. Combining these results with Theorem 7.10 and $\frac{p-2}{p-1} \geq \frac{1}{2}$, the desired inequality

$$\bar{\omega}_{\mathfrak{F}_N}^2 > \frac{1}{5N^2} \varphi(N) \log(N)$$

follows. □

REFERENCES

- [AU] *A. Abbes, E. Ullmo*: Auto-intersection du dualisant relatif des courbes modulaires $X_0(N)$. J. Reine Angew. Math. **484** (1997), 1–70. [1](#)
- [Ara] *S. J. Arakelov*: An intersection theory for divisors on an arithmetic surface. Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 1179–1192. [5.1](#)
- [Art] *M. Artin*: On isolated rational singularities of surfaces. Amer. J. Math. **88** (1966), 129–136. [3.4](#), [3.4](#)
- [BLR] *S. Bosch, W. Lütkebohmert, M. Raynaud*: Néron Models. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] **21**. Springer-Verlag, Berlin, 1990. [4](#)
- [Cin] *Z. Cinkir*: Zhang’s conjecture and the effective Bogomolov conjecture over function fields. Invent. Math. **183** (2011), 517–562. [1](#)
- [CK] *C. Curilla, U. Kühn*: On the arithmetic self-intersection number of the dualizing sheaf for Fermat curves of prime exponent, 2009, <http://arxiv.org/pdf/0906.3891>. [1](#), [5.1](#), [6.2](#), [7.1](#)
- [Cu] *C. Curilla*: Regular models of Fermat curves and applications to Arakelov theory, PhD Thesis, Universität Hamburg (2010). [1](#), [1](#), [3.16](#), [4](#)
- [De] *P. Deligne*: Intersections sur les surfaces régulières. In *SGA 7 II*. Lect. Notes Math. **340**, (1973), 1–38.
- [EH] *D. Eisenbud, J. Harris*: The Geometry of Schemes. Graduate Texts in Mathematics **197**. Springer-Verlag, New York, 2000. [2.2](#), [2.2](#)
- [Ei] *D. Eisenbud*: Commutative Algebra (with a View Toward Algebraic Geometry). Graduate Texts in Mathematics **150**. Springer-Verlag, New York, 1995. [2.1](#)
- [Gro] *A. Grothendieck*: Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. Inst. Hautes Études Sci. Publ. Math. (1965), 231. [2.1](#), [2.6](#), [4](#)
- [HW] *G. H. Hardy, E. M. Wright*: Introduction to the theory of numbers, sixth edition. Oxford University Press, Oxford, 2008. [7.1](#)
- [Hu] *C. Huneke*: Symbolic powers of prime ideals and special graded algebras. Comm. Algebra **9** (1981), 339–366. [2.2](#)
- [Ja] *A. Javanpeykar*: Polynomial bounds for Arakelov invariants of Belyi curves. Algebra Number Theory **8** (2014), 89–140. [1](#)
- [Kü2] *U. Kühn*: On the arithmetic self-intersection number of the dualizing sheaf on arithmetic surfaces, 2013, <http://arxiv.org/pdf/0906.2056>. [1](#), [1](#), [5.2](#), [5.2](#)
- [KM] *U. Kühn, J. Steffen Müller*: Lower bounds on the arithmetic self-intersection number of the relative dualizing sheaf on arithmetic surfaces, to appear in Trans. Amer. Math. Soc. [1](#), [1](#), [1](#), [5.3](#), [5.3](#)
- [La] *S. Lang*: Introduction to Arakelov Theory. Springer-Verlag, New York, 1988. [1](#), [7.2](#)
- [Lip2] *J. Lipman*: Desingularization of two-dimensional schemes. Ann. Math. (2) **107** (1978), 151–207. [2.3](#)
- [Liu] *Q. Liu*: Algebraic Geometry and Arithmetic Curves. Oxford Graduate Texts in Mathematics **6**. Oxford University Press, Oxford, 2002. [2.1](#), [2.1](#), [2.1](#), [2.2](#), [2.2](#), [2.2](#), [2.2](#), [2.3](#), [2.3](#), [3.6](#), [3.4](#), [3.4](#), [4](#), [4](#), [6.1](#), [6.2](#), [6.2](#)
- [Mat] *H. Matsumura*: Commutative ring theory. Second ed.. Cambridge Studies in Advanced Mathematics **8**. Cambridge University Press, Cambridge, 1989. [2.1](#), [2.1](#), [2.1](#), [2.14](#)
- [May] *H. Mayer*: Self-intersection of the relative dualizing sheaf on modular curves $X_1(N)$. J. Théor. Nombres Bordeaux **26** (2014), 111–161. [1](#)
- [Mc] *W. G. McCallum*: The degenerate fibre of the Fermat curve. In *Number theory related to Fermat’s last theorem* (Cambridge, Mass., 1981). Progr. Math. **26**. Birkhäuser Boston, Mass., (1982), 57–70. [1](#), [3.1](#), [3.1](#), [3.14](#)
- [MU] *P. Michel, E. Ullmo*: Points de petite hauteur sur les courbes modulaires $X_0(N)$. Invent. Math. **131** (1998), 645–674. [1](#)

- [MB] *L. Moret-Bailly*: Hauteurs et classes de Chern sur les surfaces arithmétiques. Astérisque **183** (1990), 37–58, Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). [1](#)
- [MR] *V. K. Murty, D. Ramakrishnan*: The Manin-Drinfel’d theorem and Ramanujan sums. Proc. Indian Acad. Sci. Math. Sci. **97** (1987), 251–262. [6.1](#)
- [Pa] *A. N. Parshin*: Application of ramified coverings in the theory of Diophantine equations. Mat. Sb. **180** (1989), 244–259. [1](#)
- [Ro] *D. E. Rohrlich*: Points at infinity on the Fermat curves. Invent. Math. **39** (1977), 95–127. [7.1](#)
- [So] *C. Soulé*: Géométrie d’Arakelov des surfaces arithmétiques, Séminaire Bourbaki, Vol. 1988/89. Astérisque **177-178** (1989), 327–343. [5.1](#)
- [Sz] *L. Szpiro*: Sur les propriétés numériques du dualisant relatif d’une surface arithmétique. In *The Grothendieck Festschrift, Vol. III*. Progr. Math. **88**. Birkhäuser Boston, Boston, MA, (1990), 229–246. [1](#)
- [Ul] *E. Ullmo*: Positivité et discrétion des points algébriques des courbes. Ann. of Math. **147** (1998), 167–179. [1](#)
- [Vo] *P. Vojta*: Diophantine Inequalities and Arakelov Theory. In *Introduction to Arakelov Theory* (Lang [\[La\]](#)). Springer, (1988), 155–178. [1](#)
- [Zh1] *S. Zhang*: Admissible pairing on a curve. Invent. Math. **112** (1993), 171–193. [1](#)
- [Zh2] ———: Gross-Schoen cycles and dualising sheaves. Invent. Math. **179** (2010), 1–73. [1](#)

FACHBEREICH MATHEMATIK, BEREICH AZ, UNIVERSITÄT HAMBURG, BUNDESSTRASSE 55, 20146 HAMBURG, GERMANY

E-mail address: c.curilla@web.de

INSTITUT FÜR MATHEMATIK, CARL VON OSSIETZKY UNIVERSITÄT OLDENBURG, 26111 OLDENBURG, GERMANY

E-mail address: jan.steffen.mueller@uni-oldenburg.de